

POLYNOMIAL TYPE ALGEBRAIC COMPLEXITIES AND ELUSIVE FUNCTIONS

HÔNG VÂN LÊ

ABSTRACT. We introduce a general concept of complexity and a polynomial type algebraic complexity of a polynomial mapping. The notion of polynomial type algebraic complexity encompasses the determinantal complexity. We analyze the relation between polynomial type algebraic complexities and elusive functions. We study geometric-algebraic properties of polynomial type computational complexities. We present two algorithms to construct a test function for estimating a polynomial type algebraic complexity; one of them is based on Gröbner bases, the other uses the resultant of polynomials in many variables. We describe an algorithm to compute a polynomial type algebraic complexity of polynomial mappings defined over \mathbb{C} . We develop the method by Kumar-Lokam-Patankar-Sarma that uses the effective elimination theory combined with algebraic number field theory in order to construct elusive functions and polynomial mappings with large circuit size. For $\mathbb{F} = \mathbb{C}$ or \mathbb{R} , and for any given r , we construct explicit examples of sequences of polynomial mappings $f_n : \mathbb{F}^{2n} \rightarrow \mathbb{F}^n$ and of degree $5r+1$ whose coefficients are algebraic numbers such that any depth r arithmetic circuit for f_n is of size greater than $n^2/(50r^2)$. Using the developed methods we also construct concrete examples of polynomials with large determinantal complexity.

AMSC: 03D15, 68Q17, 13P25

CONTENTS

1. Introduction	2
2. Complexity and polynomial type algebraic complexities	4
3. Elusive functions and associated polynomial type algebraic complexities	11
4. Zariski closure of the image of a polynomial mapping, effective elimination theory and algebraic number field theory	17

Partially supported by the MSMT project “Eduard Čech Center” and RVO: 67985840.

Address: Institute of Mathematics of ASCR, Žitná 25, 11567 Praha,
email: hvle@math.cas.cz.

5. Algorithms to compute and to estimate polynomial type algebraic complexities	21
6. Examples and applications	24
7. Conclusions	31
Acknowledgements	31
References	32

1. INTRODUCTION

In computational algebraic complexity theory we investigate different complexity classes of sequences (f_n) of polynomials over a field \mathbb{F} . We also search lower or upper bounds of complexities on a given polynomial.

Two most important complexities of a multivariate polynomial f are the circuit complexity $L(f)$ and the formula size $L_e(f)$. These complexities measure the minimal size of certain arithmetic circuits computing f . Arithmetic circuits are the standard computational model for computing polynomials. An *arithmetic circuit*, as defined, e.g., in [13, §1.1], is a finite directed acyclic graph whose nodes are divided into four types: nodes of in-degree 0 (input gates) labelled with an input variable or the field element 1, nodes labelled with $+$ (sum gates), node labelled with \times (product gates), and nodes of out-degree 0 (output gates) giving the result of the computation. Every edge (u, v) in the graph is labelled with a field element α . It computes the product of α with the polynomial computed by u . A product gate (resp. a sum gate) computes the product (resp. the sum) of polynomials computed by the edges that reach it. We say that a polynomial $f \in \mathbb{F}[X_1, \dots, X_n]$ is computed by a circuit if it is computed by one of the circuit output gates. If a circuit has m output gates, then it computes a m -tuple of polynomials $f^i \in \mathbb{F}[X_1, \dots, X_n]$, $i \in [1, m]$. In what follows we consider only ordered m -tuples of polynomials resulting from a numeration of the output gates of an arithmetic circuit; so an m -tuple is understood as an ordered m -tuple. Further, assuming in this note that \mathbb{F} is a field of characteristic 0, we also identify an m -tuple of polynomials in n variables with a polynomial mapping from \mathbb{F}^n to \mathbb{F}^m . Let us denote by $\text{Pol}^r(\mathbb{F}^n, \mathbb{F}^m)$ the space of all polynomial mapping of degree at most r from \mathbb{F}^n to \mathbb{F}^m and set $\text{Pol}(\mathbb{F}^n, \mathbb{F}^m) := \cup_{r=0}^{\infty} \text{Pol}^r(\mathbb{F}^n, \mathbb{F}^m)$.

We define *the size of a circuit* as the number of its edges, and *the circuit complexity* of a polynomial mapping f to be the minimum size of an arithmetic circuit computing f [13]. *The formula size $L_e(f)$ of a polynomial mapping f* is defined as the minimum size of an arithmetic

circuit computing f , which is a directed tree, i.e., all vertices have out-degree at most 1.

The formula size and the circuit complexity of polynomial mappings do not have clear geometric or algebraic structure. In [16] Valiant suggested to “approximate” the formula size of a polynomial by the determinantal complexity, observing that on the one hand, the determinantal complexity is a lower bound for the formula size, and on the other hand, the determinantal complexity has a clear algebraic and geometric interpretation. Geometric and algebraic properties of the determinantal complexity of a polynomial have been employed by Mignon-Ressayre [11] and by Mulmuley-Sohoni [12] to study lower bounds on the determinantal complexity, and to attack the problem VP versus VNP .

In [13] Raz proposed a geometric approach to obtain a lower bound on the circuit complexity of a polynomial by introducing a polynomial mapping associated with the graph of a given arithmetic circuit. Motivated by his approach, we introduce in this note a general concept of computational complexity and a concept of polynomial type computational complexity. We also analyze the relation between polynomial type algebraic complexities and elusive functions. Further, we study geometric-algebraic properties of polynomial type algebraic complexities. Our aim is to show that the notion of polynomial type algebraic complexities is well motivated, moreover, these complexities have good geometric and algebraic properties. For example, there are algorithms to compute or estimate them under some mild conditions (Remark 2.6, Theorem 5.1, Remark 5.6.1).

The structure of our note is as follows. In section 2 we introduce the notions of complexity and polynomial type algebraic complexity of a polynomial mapping. We show that polynomial type algebraic complexities have nice algebraic structure (Remark 2.6) and that the determinantal complexity is a polynomial type algebraic complexity (Example 2.7). We give an example of a polynomial type algebraic complexity associated with a universal circuit graph (Example 2.11). In section 3 we recall the notion of a (s, r) -elusive function introduced by Raz in [13]. To study (s, r) -elusive functions we introduce the notion of a (s, r) -elusive subset (Definition 3.2) and we characterize polynomial mappings whose image contains an (s, r) -elusive subset consisting of k -points (Corollary 3.5). This construction leads to the notions of a (s, r, k) -elusive function and of a strong (s, r) -elusive function (Definitions 3.2, 3.9). We compare these notions, using an interpolation formula for polynomial mappings (Proposition 3.6, Remark 3.10). In

section 4 we develop the method invented by Kumar-Lokam-Patankar-Sarma [9] that uses the effective elimination theory combined with algebraic number field theory in order to find concrete points b which lie outside the image of a polynomial mapping g , if g is defined over \mathbb{Q} , such that the coordinates of b are algebraic numbers (Proposition 4.5). In section 5 we describe an algorithm, based on Gröbner bases, to compute polynomial type algebraic complexity over \mathbb{C} (Theorem 5.1). We propose two algorithms to construct a test function for estimating a polynomial type algebraic complexity. A test function T_α , $\alpha \in \mathbb{N}$, for estimating a polynomial type computational complexity $C_S(f)$ is a polynomial on a vector space $Pol^k(\mathbb{F}^n) \ni f$ of polynomials in variables X_1, \dots, X_n and of degree k such that $T_\alpha(f) \geq 0$ implies $C_S(f) \geq \alpha$. Our algorithms exploit the notion of algebraic dependence of a sequence of multivariate polynomials. The first algorithm uses Gröbner basis for finding generators of the ideal of the algebraic closure of the image of a polynomial mapping (Remark 4.1, Proposition 5.4). The second algorithm shows that the resultant of polynomials in many variables can serve as a test function for estimating polynomial type algebraic complexities (Proposition 5.5, Remark 5.6.1). In section 6 we show some examples and applications of our methods. We construct examples of polynomials of large determinantal complexity (Example 6.2) and examples of (s, r) -elusive functions (Proposition 6.6). Using this we construct explicit examples of sequences of polynomials f_n of n -variable and degree $5r$ whose coefficients are algebraic numbers such that any depth r arithmetic circuit for f_n over \mathbb{R} or \mathbb{C} is of size greater than $n^2/50r^2$ (Proposition 6.9).

Finally we note that our results obtained for polynomial type algebraic complexities are applicable for similar complexities of the same nature, e.g. the rank of tensors and the rigidity of matrices.

2. COMPLEXITY AND POLYNOMIAL TYPE ALGEBRAIC COMPLEXITIES

In this section we examine several important complexities and computational models, and based on these examples we introduce the notion of complexity and polynomial type algebraic complexity of a polynomial mapping (Definition 2.1 and Definition 2.5). We show that the determinantal complexity is a polynomial type algebraic complexity (Example 2.7). We introduce the notion of normal circuit size, which is a polynomial type algebraic complexity associated with a universal circuits graph (Example 2.11), and we explain the relationship between normal circuit size and circuit size (Remark 2.12).

Definition 2.1. 1. A *computational model* M for computing a polynomial mapping $f = (f^1, \dots, f^m) \in \text{Pol}(\mathbb{F}^n, \mathbb{F}^m)$ is an algorithm transforming an n -tuple of variables (X_1, \dots, X_n) to the m -tuple (f^1, \dots, f^m) .

2. Let $\mathcal{C}(f)$ be a class of computational models for computing a polynomial mapping $f \in \text{Pol}(\mathbb{F}^n, \mathbb{F}^m)$ and \leq_c a partial ordering on $\mathcal{C}(f)$. A function $S : \mathcal{C}(f) \rightarrow \mathbb{N}$ is called a *complexity function*, if the following natural condition holds

$$(2.1) \quad S(M) \leq S(M') \text{ if } M \leq_c M'.$$

A complexity function $S : \mathcal{C}(f) \rightarrow \mathbb{N}$ defines *the complexity* $C_S(f)$ of f as follows

$$(2.2) \quad C_S(f) := \min\{S(M) \mid M \in \mathcal{C}(f)\}.$$

Remark 2.2. 1. Usually one considers a family \mathcal{F} of polynomials $f \in \text{Pol}(\mathbb{F}^n, \mathbb{F}^m)$, where m and n need not be constant, and studies computational models for computing elements in this family. The complexity function S is then required to be defined on the whole family of computational models for computing elements of the family \mathcal{F} . In this family situation, the complexity $C_S(f)$ of $f \in \mathcal{F}$ is also defined by (2.2). Thus, the definition of a complexity of a polynomial mapping in \mathcal{F} does not depend on the parametrization of the family.

2. In [17], [4] the authors used “program” in their definition of a computational model, which has the same meaning as “algorithm” in our definition, except that we do not require to write explicitly all elementary instructions in an algorithm. Our concept of a complexity of a computational model is more general than their concepts of a complexity of a computational model, which is supposed to be to the length of the program (i.e., the number of the operations in the program).

Example 2.3. An arithmetic circuit computing a polynomial mapping $f \in \text{Pol}(\mathbb{F}^n, \mathbb{F}^m)$ is a computational model of f . There is a natural partial ordering \leq_c on the set of arithmetic circuits defined as follows. For an arithmetic circuit Ψ let Γ_Ψ^0 be the underlying graph without label of nodes and of edges. Then the partial ordering $\Psi \leq_c \Psi'$ holds if and only if there is an embedding Γ_Ψ^0 in $\Gamma_{\Psi'}^0$. Clearly, the circuit complexity and the formula size of a polynomial mapping are most important cases of the notion of a complexity in Definition 2.1.

Example 2.4. In this example we show that the determinantal complexity defined by Mignon and Ressayre [11], generalizing the Valiant concept in [16], is also a complexity in the sense of Definition 2.1. Let us first fix necessary notations and definitions.

- Let $Det_m \in \mathbb{F}[X_1, \dots, X_{m^2}]$ denote the determinantal polynomial, i.e., $Det_m(a) := \det a$ for $a \in \mathbb{F}^{m^2} = Mat_m(\mathbb{F})$.
- Let Aff_{n,m^2} denote the space of all affine maps from \mathbb{F}^n to \mathbb{F}^{m^2} .
- A pair $[A, Det_m]$, $A \in \text{Aff}_{n,m^2}$, is said to be a *computational model for computing a polynomial* $f \in \mathbb{F}[X_1, \dots, X_n]$, if $f = A^* Det_m$, or equivalently $f(a_1, \dots, a_n) = Det_m(A(a_1, \dots, a_n))$ for any input $(a_1, \dots, a_n) \in \mathbb{F}^n$.
- For a polynomial $f \in \mathbb{F}[X_1, \dots, X_n]$ set

$$\mathcal{C}(f) := \bigcup_{m=0}^{\infty} \{[A, Det_m] \mid A^* Det_m = f, A \in \text{Aff}_{n,m^2}\}.$$

We define the complexity function $S : \mathcal{C}(f) \rightarrow \mathbb{N}$ by

$$(2.3) \quad S([A, Det_m]) := m.$$

- The *determinantal complexity* $c_{\det}(f)$ of a polynomial $f \in \mathbb{F}[X_1, \dots, X_n]$ is defined as follows (cf. [11] and (2.2))

$$(2.4) \quad c_{\det}(f) := \min\{S(M) \mid M \in \mathcal{C}(f)\}.$$

The set $\mathcal{C}(f)$ is not empty, and therefore the determinantal complexity is well-defined, thanks to the Valiant result [16], which states that $c_{\det}(f) \leq 2L_e(f)$.

Unlike the circuit complexity or the formula size, the determinantal complexity has nice geometric-algebraic properties, which we now explain.

We now abbreviate $Pol^k(\mathbb{F}^n, \mathbb{F})$ as $Pol^k(\mathbb{F}^n)$. We consider a sequence of polynomial mappings

$$\mathcal{D}_{n,m} : \text{Aff}_{n,m^2} \rightarrow \mathbb{F}[X_1, \dots, X_m], A \mapsto A^* Det_m, 0 \leq m < \infty.$$

By the Valiant theorem [16], for any k , there exists a finite number $N(k)$ such that

$$Pol^k(\mathbb{F}^n) = \bigcup_{0 \leq m \leq N(k)} \mathcal{D}_{n,m}(\text{Aff}_{n,m^2}).$$

Note that there is a canonical embedding $Mat_{m-1}(\mathbb{F}) \rightarrow Mat_m(\mathbb{F})$ corresponding to the decomposition $\mathbb{F}^m = \mathbb{F}^{m-1} \oplus \mathbb{F}$. Since the restriction of \det_m to $Mat_{m-1}(\mathbb{F})$ is equal to \det_{m-1} we get the following inclusions

$$(2.5) \quad \mathcal{D}_{n,1}(\text{Aff}_{n,1}) \subset \dots \subset \mathcal{D}_{n,N(k)}(\text{Aff}_{n,N(k)^2}) = Pol^k(\mathbb{F}^n).$$

It is easy to see that for $f \in \mathbb{F}[X_1, \dots, X_m]$, (2.4) is equivalent to the following equation

$$(2.6) \quad c_{\det}(f) := \min\{m \mid f \in \mathcal{D}_{n,m}(\text{Aff}_{n,m^2})\}.$$

Now we shall introduce the notion of polynomial type complexity, generalizing the formula (2.6).

Definition 2.5. Let $\mathcal{F} \subset \text{Pol}(\mathbb{F}^n, \mathbb{F}^m)$ be a family of polynomial mappings and $\mathcal{C}(\mathcal{F})$ a family of computational model for computing elements in \mathcal{F} . Let $\pi : \mathcal{C}(\mathcal{F}) \rightarrow \mathcal{F}$ denote the assignment to each computational model its output. A complexity function S on $\mathcal{C}(\mathcal{F})$ is called *of polynomial type*, if

- there is a family of vector spaces $\{V_\alpha \mid \alpha \in \mathcal{A} \subset \mathbb{N}\}$ together with a polynomial mapping $\widehat{\mathcal{P}}_\alpha : V_\alpha \rightarrow \text{Pol}^{K(\alpha)}(\mathbb{F}^n, \mathbb{F}^m)$, $K(\alpha) < \infty$, such that

$$(2.7) \quad V_\alpha \subset V_{\alpha'} \text{ if } \alpha \leq \alpha',$$

$$(2.8) \quad \widehat{\mathcal{P}}_\alpha(V_\alpha) \subset \widehat{\mathcal{P}}_\beta(V_\beta) \text{ if } \alpha \leq \beta;$$

- there is a mapping

$$\Pi : \mathcal{C}(\mathcal{F}) \rightarrow \bigcup_{\alpha \in \mathcal{A}} V_\alpha$$

such that the following diagram is commutative

$$(2.9) \quad \begin{array}{ccc} \mathcal{C}(\mathcal{F}) & \xrightarrow{\Pi} & \bigcup_{\alpha} V_\alpha \\ \downarrow \pi & & \downarrow \widehat{\mathcal{P}}_\alpha \\ \mathcal{F} & \hookrightarrow & \text{Pol}(\mathbb{F}^n, \mathbb{F}^m) \end{array} \quad ;$$

- for all $f \in \mathcal{F}$ and for each $M \in \mathcal{C}(f) \subset \mathcal{C}(\mathcal{F})$ we have

$$(2.10) \quad S(M) = \min\{\alpha \in \mathcal{A} \mid \Pi(M) \in V_\alpha \text{ and } \widehat{\mathcal{P}}_\alpha(\Pi(M)) = f\}.$$

An algebraic complexity C_S is called *of polynomial type*, if the associated complexity function S is of polynomial type.

Remark 2.6. 1. Formula (2.10) implies that the polynomial type algebraic complexity C_S defined by a polynomial type complexity function S satisfies

$$(2.11) \quad C_S(f) = \min\{\alpha \mid f \in \widehat{\mathcal{P}}_\alpha(V_\alpha)\},$$

which is a generalization of (2.6).

2. Taking into account (2.11) we note that the compatibility conditions (2.7) and (2.8) ensure that the set of polynomial mappings of complexity α is a subset of the set of polynomial mappings of complexity β , if $\alpha \leq \beta$.

Example 2.7. In Example 2.4 we explained how the notion of determinantal complexity fits into our concept of a complexity. Now we show that the determinantal complexity is a polynomial type algebraic complexity. For a polynomial $f \in \mathbb{F}[X_1, \dots, X_n]$ let

$$C(f) = \{[A, Det_p] \mid p \in \mathbb{N}, A \in \text{Aff}_{n,p^2} \text{ and } f = A^* Det_p\}$$

be a computational model for computing f . We set $\mathcal{A} := \mathbb{N}$ and

- $V_p = \text{Aff}_{n,p^2}$ for $p \in \mathcal{A}$.
- $\Pi : \{C(f) \mid f \in \text{Pol}^m(\mathbb{F}^n)\} \rightarrow \cup_p V_p, [A, Det_p] \mapsto A$.
- $\widehat{P}_p := \mathcal{D}_{n,p} : V_p \rightarrow \text{Pol}^p(\mathbb{F}^n)$.

Clearly, the diagram (2.9) for the defined Π , \widehat{P}_p , and π is commutative. Relation (2.5) is specialization of (2.7) and (2.8). Finally (2.3) and (2.6) are specialization of (2.10) and (2.11). Thus all the conditions in Definition 2.5 hold for this case.

The remainder of this section is devoted to constructing an example of a polynomial type algebraic complexity whose associated computational models are arithmetic circuits supplied with the natural partial ordering \leq_c . Our construction is based on Raz's result in [13]. Let us recall definitions in [13, §2], which are needed for our construction.

- A *circuit graph* G is the underlying graph G_Φ of an arithmetic circuit Φ together with the labels of all nodes. This is the entire circuit, except for the labels of the edges. We call $G = G_\Phi$ *the circuit graph* of Φ .
- For a circuit graph G , *the size* of G is the number of its edges, denoted by $\text{Size}(G)$, and *the depth* of G is the length of the longest directed path in G , and denoted by $\text{Depth}(G)$.
- *The syntactic degree* of a node in a circuit graph G is defined inductively as follows. The syntactic degree of an input gate (i.e., a node of in-degree 0) is zero if it is labelled by the field element 1, and 1 if it is labelled by an input variable. The syntactic degree of a sum gate is the maximum of the syntactic degrees of its children. The syntactic degree of a product gate is the sum of the syntactic degrees of its children. The syntactic degree of a circuit graph is the maximal syntactic degree of a node in the circuit.

The meaning of the syntactic degree of a circuit graph is explained by the following obvious Lemma, whose proof is omitted.

Lemma 2.8. *Suppose that G_Φ is a circuit graph of an arithmetic circuit Φ computing a polynomial mapping. The maximal degree of the*

polynomial mapping computed by an arithmetic circuit Φ' with the same circuit graph G_Φ is the syntactic degree of G_Φ .

Assume that G is a circuit graph of ordered edges denoted by y_1, \dots, y_s and of syntactic degree r with n input variables X_1, \dots, X_n and with m output gates g_1, \dots, g_m . For any s -tuple (a_1, \dots, a_s) of elements $a_i \in \mathbb{F}$, we define a circuit $\Phi_G(a_1, \dots, a_s)$ by replacing the notations y_1, \dots, y_s in G by the field elements a_1, \dots, a_s as the labels for the corresponding edges. By Lemma 2.8 the circuit $\Phi_G(a_1, \dots, a_s)$ computes an m -tuple (g_1, \dots, g_m) of polynomials $g_i \in \text{Pol}^r(\mathbb{F}^n)$. Set $d(r, n, m) := m \dim \text{Pol}^r(\mathbb{F}^n) = \dim \text{Pol}^r(\mathbb{F}^n, \mathbb{F}^m)$. Fix a linear isomorphism $H_{n,m}^r : \text{Pol}^r(\mathbb{F}^n, \mathbb{F}^m) \rightarrow \mathbb{F}^{d(r,n,m)}$. We define a mapping $\Gamma_G : \mathbb{F}^s \rightarrow \mathbb{F}^{d(r,n,m)}$ by setting [13, §3.2]

$$(2.12) \quad \Gamma_G(a_1, \dots, a_s) := H_{n,m}^r(g_1, \dots, g_m) \in \mathbb{F}^{d(r,n,m)}.$$

In [13, §3.2] Raz noticed that Γ_G is a polynomial mapping in both input variables y_1, \dots, y_s and input variables X_1, \dots, X_n . The degree of a polynomial mapping Γ_G depends on G , see e.g. [13, Proposition 3.2].

The following Lemma is a direct consequence of (2.12), so we omit its proof.

Lemma 2.9. (cf. [13, Prop. 3.1, Prop. 5.1]) *Suppose that Φ is an arithmetic circuit computing $g = (g_1, \dots, g_m) \in \text{Pol}^r(\mathbb{F}^n, \mathbb{F}^m)$ such that $G_\Phi = G$. Then (2.12) holds. In particular, $H_{n,m}^r(g_1, \dots, g_m)$ belongs to the image of Γ_G .*

In [13] Raz introduced the notion of a *homogeneous arithmetic circuit* to deal with the important class of homogeneous polynomial mappings. Recall that a polynomial mapping $f \in \text{Pol}(\mathbb{F}^n, \mathbb{F}^m)$ is called *homogeneous of degree k* , if for all $a \in \mathbb{F}$ and for all $x \in \mathbb{F}^n$ we have $f(ax) = a^k f(x)$. We say that a circuit graph G is *homogeneous* if for each sum gate v in G the syntactic degree of every child of v is the same. We say that an arithmetic circuit is *homogeneous*, if the circuit graph G_Φ is homogeneous.

Theorem 2.10. [13, Proposition 2.8] *For any integers $n, s, r \geq 1$ such that $s \geq n$, there is a homogeneous circuit graph $G_{r,s,n}$ with at most $O(s \cdot r^4)$ nodes, that is universal for n -inputs and n -outputs circuits of size s that compute homogeneous polynomials of degree r , in the following sense.*

Let \mathbb{F} be a field. Let Ψ be an arithmetic circuit of size s for computing $g \in \text{Pol}^r(\mathbb{F}^n, \mathbb{F}^n)$. Then there exists an arithmetic circuit Ψ for computing g such that $G_\Psi = G_{r,s,n}$.

We call a homogeneous arithmetic circuit (r, s, n) -universal, if its circuit graph is universal for n -inputs and n -outputs circuits of size s that compute homogeneous polynomials of degree r in sense of Theorem 2.10. Given an (r, s, n) -universal homogeneous circuit graph G with ordered edges $y_1, \dots, y_{k(r,s,n)}$, any (r, s, n) -universal homogeneous arithmetic circuit whose underlying circuit graph is G has the form $\Phi_G(a_1, \dots, a_{k(r,s,n)})$, where $a_i \in \mathbb{F}$.

Denote by $Pol_{hom}(\mathbb{F}^n, \mathbb{F}^m)$ (resp. by $Pol_{hom}^r(\mathbb{F}^n, \mathbb{F}^m)$) the space of homogeneous polynomial mappings (resp. that of degree r) from \mathbb{F}^n to \mathbb{F}^m . In Example 2.11 below, using Theorem 2.10 we introduce a new polynomial type algebraic complexity of a homogeneous polynomial $g \in Pol_{hom}(\mathbb{F}^n, \mathbb{F}^n)$.

Example 2.11. For $r, s \in \mathbb{N}^+$ set

$$\mathcal{C}_n^r := \{\Phi_{G_{r,s,n}}(a_1, \dots, a_{k(r,s,n)}) \mid s \in \mathbb{N}, a_i \in \mathbb{F}\}$$

be a family of computational models. Let $\hat{\Phi}$ denote the output of an arithmetic circuit Φ . Set

- $\mathcal{A} := \mathcal{A}_n^r := \{k(r, s, n) \mid s \in \mathbb{N}\}$, $V_\alpha := \mathbb{F}^\alpha$,
- $\Pi : \mathcal{C}_n^r \rightarrow \cup_{s \in \mathbb{N}} V_s$, $(\Phi_{G_{r,s,n}}(a_1, \dots, a_{k(r,s,n)})) \mapsto (a_1, \dots, a_{k(r,s,n)})$,
- $\hat{P}_\alpha^r(a_1, \dots, a_{k(r,s,n)}) := \Gamma_{G_{r,s,n}}(a_1, \dots, a_{k(r,s,n)}) \in Pol_{hom}^r(\mathbb{F}^n, \mathbb{F}^n)$,
- $L_{nor}(f) := \min\{\alpha \mid f \in \hat{P}_\alpha^r(V_\alpha)\}$ for $f \in Pol_{hom}^r(\mathbb{F}^n, \mathbb{F}^n)$.

By Lemma 2.9 $\hat{P}_s^r \circ \Pi(\Phi_{G_{r,s,n}}(a_1, \dots, a_{k(r,s,n)})) = \pi(\Phi_{G_{r,s,n}}(a_1, \dots, a_{k(r,s,n)}))$. Thus the diagram (2.9) for Example 2.11 is commutative. We call $L_{nor}(f)$ the normal circuit size of $f \in Pol_{hom}^r(\mathbb{F}^n, \mathbb{F}^n)$. By (2.8) and (2.11) the normal circuit size of a homogeneous polynomial mapping $f \in Pol_{hom}^r(\mathbb{F}^n, \mathbb{F}^n)$ is a polynomial type algebraic complexity.

Remark 2.12. Let Φ be a $(r, L(f), n)$ -universal circuit computing a polynomial mapping $f \in Pol_{hom}^r(\mathbb{F}^n, \mathbb{F}^n)$. Since Φ computes f , we have

$$(2.13) \quad L(f) \leq Size(G_\Phi).$$

Observing that for fixed (r, n) the function $s \mapsto k(r, s, n)$ is a monotone function, we have $Size(G_\Phi) = L_{nor}(f)$. On the other hand, by Raz's result [13, Proposition 2.8], see also Theorem 2.10 above,

$$(2.14) \quad Size(G_\Phi) = O(L(f)^2 r^8).$$

(2.13) and (2.14) imply that a sequence of circuit sizes $L(f_{q(r,n)})$ of polynomial mappings $f_{q(r,n)} \in Pol_{hom}^r(\mathbb{F}^n, \mathbb{F}^n)$ has super-polynomial growth, if the sequence $L_{nor}(f_{q(r,n)})$ has super-polynomial growth.

Note that it is not easy to find explicitly the polynomial mappings \hat{P}_k^r . It is also hard to estimate the coefficients of \hat{P}_k^r . In [13] Raz

proposed to study (s, r) -elusive polynomial mappings, which could give us a method to understand circuit size without investigation of the normal circuit size. We will show in the next section that the notion of a (s, r) -elusive function is also closely related with another polynomial type algebraic complexity (Remark 3.10 and Definition 3.11).

3. ELUSIVE FUNCTIONS AND ASSOCIATED POLYNOMIAL TYPE ALGEBRAIC COMPLEXITIES

In this section we recall the notion of a (s, r) -elusive function introduced by Raz in [13] for constructing sequences of multivariate polynomials of high circuit complexity (Definition 3.1). To study (s, r) -elusive functions we introduce the notion of a (s, r) -elusive subset (Definition 3.2) and we find a condition for a polynomial mapping whose image contains a (s, r) -elusive subset (Corollary 3.5). We also introduce the notion of a (s, r, k) -elusive function (Definition 3.2) and the notion of a strong (s, r) -elusive functions (Definition 3.9). The last one leads to the notion of a polynomial type algebraic complexity for non-constant polynomial mappings (Remark 3.10, Definition 3.11). We compare (s, r) -elusive functions, (s, r, k) -elusive functions and strong (s, r) -elusive functions, using an interpolation formula for polynomial mappings over \mathbb{F} and an evaluation mapping (Proposition 3.6, Remark 3.10).

Definition 3.1 ([13], p. 2). A polynomial mapping $f : \mathbb{F}^n \rightarrow \mathbb{F}^m$ is called (s, r) -*elusive*, if for every polynomial mapping $\Gamma : \mathbb{F}^s \rightarrow \mathbb{F}^m$ of degree r , we have $f(\mathbb{F}^n) \not\subset \Gamma(\mathbb{F}^s)$.

Using the existence of elusive functions Raz has constructed polynomials of large circuit size [13, §3.4]. Raz's construction of elusive functions is based on a certain combinatoric property of the coefficients of a special polynomial mapping [13, Lemma 4.1]. Our approach to elusive functions is based on the concept of an (s, r) -elusive subset.

Definition 3.2. A k -tuple S_k of k points in \mathbb{F}^m is called (s, r) -*elusive*, if for every polynomial mapping $\Gamma : \mathbb{F}^s \rightarrow \mathbb{F}^m$ of degree r , we have $S_k \not\subset \Gamma(\mathbb{F}^s)$. A polynomial mapping $f : \mathbb{F}^n \rightarrow \mathbb{F}^m$ is called (s, r, k) -*elusive*, if there is a k -tuple of points in the image $f(\mathbb{F}^n)$ which is (s, r) -elusive.

Clearly any (s, r, k) -elusive function is (s, r) -elusive.

Example 3.3. (cf. [13]) A polynomial mapping $f : \mathbb{F}^n \rightarrow \mathbb{F}^m$ is $(m-1, 1)$ -elusive, if and only if the image $f(\mathbb{F}^n)$ does not belong to any hyperplane in the affine space \mathbb{F}^m . Equivalently, a $(m-1, 1)$ -elusive

polynomial is $(m-1, 1, m+1)$ -elusive. For example, the moment curve $f : \mathbb{C} \rightarrow \mathbb{C}^m, t \mapsto (t, t^2, \dots, t^m)$ is $(m-1, 1)$ -elusive, since the image of the moment curve contains $m+1$ points $b_0 := f(0) = 0, \dots, b_i := f(a_i) \in \mathbb{C}^m, 1 \leq i \leq m$, satisfying the following condition. The values $a_i \in \mathbb{F}^n$ are chosen such that b_1, \dots, b_m are non-zero linear independent vectors in \mathbb{C}^n . Clearly the $(m+1)$ -tuple $(0, b_1, \dots, b_m)$ is $(m-1, 1)$ -elusive, which implies that f is $(m-1, 1, m+1)$ -elusive, see Corollary 3.7 for a detailed explanation.

To treat (s, r) -elusive k -tuples we consider the following evaluation map

$$(3.1) \quad \begin{aligned} Ev_{r,s,m}^k : Pol^r(\mathbb{F}^s, \mathbb{F}^m) \times (\mathbb{F}^s)^k &\rightarrow (\mathbb{F}^m)^k, \\ (f_1, \dots, f_m)(a_1, \dots, a_k) &\mapsto (f_1(a_1), \dots, f_m(a_k)), \end{aligned}$$

where $f_j \in Pol^r(\mathbb{F}^s)$ for $1 \leq j \leq m$ and $a_i \in \mathbb{F}^s$ for $1 \leq i \leq k$.

We identify a k -tuple $S_k = (b_1, \dots, b_k)$, $b_i \in \mathbb{F}^m$, with the point $\overline{S_k} \in (\mathbb{F}^m)^k$ whose coordinate $\overline{S_k}^{i,j}$, $1 \leq i \leq s, 1 \leq j \leq m$, is equal to the i -th coordinate b_j^i of $b_j \in \mathbb{F}^m$.

Lemma 3.4. *A k -tuple $S_k \subset \mathbb{F}^m$ is (s, r) -elusive, if and only if $\overline{S_k}$ does not belong to the image of $Ev_{r,s,m}^k$.*

Proof. Assume that $\overline{S_k}$ belongs to the image of $Ev_{r,s,m}^k$. Then there are a polynomial mapping $f \in Pol^r(\mathbb{F}^s, \mathbb{F}^m)$ and a point $a \in \mathbb{F}^{sk}$ such that

$$(3.2) \quad Ev_{r,s,m}^k(f, a) = \overline{S_k}.$$

We write $S_k = (b_1, \dots, b_k)$, $b_i \in \mathbb{F}^m$, and $a = (a_1, \dots, a_k)$, $a_i \in \mathbb{F}^s$. The equation (3.2) implies

$$(3.3) \quad f(a_i) = b_i.$$

Thus $S_k \subset f(\mathbb{F}^s)$. This proves the “only if” assertion of Lemma 3.4.

Conversely, assume that $S_k \subset f(\mathbb{F}^s)$ for some $f \in Pol^r(\mathbb{F}^s, \mathbb{F}^m)$. Then there are points $a_i \in \mathbb{F}^s, i = \overline{1, k}$, such that (3.3) holds for all i . Since (3.3) is equivalent to (3.2), it follows that $\overline{S_k}$ does not belong to the image of $Ev_{r,s,m}^k$. This completes the proof of Lemma 3.4. \square

Corollary 3.5. *A polynomial map $f : \mathbb{F}^n \rightarrow \mathbb{F}^m$ is (s, r, k) -elusive, if and only if the subset $\hat{f}^k := f(\mathbb{F}^n) \times \dots \times_{k \text{ times}} f(\mathbb{F}^n) \subset \mathbb{F}^{mk}$ does not belong to the image of the evaluation mapping $Ev_{s,r,m}^k$.*

Now we are going to find a sufficient condition for a polynomial mapping $f : \mathbb{F}^n \rightarrow \mathbb{F}^m$ to be (s, r, k) -elusive using an interpolation formula for a polynomial mapping.

Interpolation of a function in many variables by a polynomial mapping has been investigated for a long time, but there are many interesting and unsolved questions [7]. One of the main differences between interpolation of a function in one variable and interpolation of a function in many variables is that in the former case an interpolable set, i.e., the set at which the value of an interpolating polynomial function (resp. a polynomial mapping) must coincide with the value of a given interpolable function, can be arbitrary, but in the later case cannot be arbitrary. The interpolation formula given below is likely unknown, though possibly, there are some similar formulas. Our interpolable set is a lattice in a simplex in \mathbb{F}^n .

Note that a monomial $X_1^{i_1} \cdots X_s^{i_s} \in \text{Pol}^r(\mathbb{F}^s)$ can be identified with an ordered s -tuple (i_1, \dots, i_s) of non-negative integers i_j , $1 \leq j \leq s$, such that $i_1 + \dots + i_s \leq r$. The following formula is well-known

$$(3.4) \quad \dim \text{Pol}^r(\mathbb{F}^s) = \binom{s+r}{s}.$$

By (3.4) there exists a 1-1 mapping H_s^r from the set Mon_s^r of all monomials $X_1^{i_1} \cdots X_s^{i_s} \in \text{Pol}^r(\mathbb{F}^s)$ to the set $S_{s,r}$ of $\binom{s+r}{r}$ points $(i_1, \dots, i_s) \in \mathbb{F}^s$. (The mapping H_s^r induces a linear isomorphism $H_{s,m}^r : \text{Pol}^r(\mathbb{F}^s, \mathbb{F}^m) \rightarrow (\mathbb{F}^s)^m$, $k = m \binom{s+r}{r}$ used in Lemma 2.9.) For a set $S_{s,r,m}$ of $\binom{s+r}{r}$ points in \mathbb{F}^m we numerate the points in $S_{s,r,m}$ by b_{i_1, \dots, i_s} , where $i_s \in \mathbb{N}$ and $\sum_s i_s \leq r$.

Now we are ready to prove

Proposition 3.6. *Given a tuple $S_{s,r,m}$ of $\binom{s+r}{r}$ points b_{i_1, \dots, i_s} in \mathbb{F}^m , $i_j \in \mathbb{N}$ and $\sum_{j=1}^s i_j \leq r$, there exists an algorithmically constructed polynomial mapping $f_{S_{s,r,m}} : \mathbb{F}^s \rightarrow \mathbb{F}^m$ of degree r such that*

$$(3.5) \quad f_{S_{s,r,m}}(i_1, \dots, i_s) = b_{i_1, \dots, i_s},$$

for all $(i_1, \dots, i_s) \in \mathbb{N}^s \subset \mathbb{F}^s$ satisfying $\sum_{j=1}^s i_j \leq r$.

Proof. Let f^i (resp. b^i) denote the i -th coordinate of a polynomial mapping $f : \mathbb{F}^s \rightarrow \mathbb{F}^m$ (resp. of a point $b \in \mathbb{F}^m$), i.e., $f = (f^1, \dots, f^m)$. Note that (3.5) is equivalent to the following system of equations

$$(3.6) \quad f_{S_{s,r,m}}^i(i_1, \dots, i_s) = b_{i_1, \dots, i_s}^i, \text{ for } i \in [1, m]$$

and for all $(i_1, \dots, i_s) \in \mathbb{N}^s \subset \mathbb{F}^s$ satisfying $\sum_s i_s \leq r$. Comparing (3.5) with (3.6) we can assume without loss of generality that $m = 1$.

We construct $f_{S_{s,r,1}}$ by induction on s . Note that the case $s = 1$ is well-known. Given an $(r+1)$ -tuple (b_0, \dots, b_r) of elements $b_i \in \mathbb{F}$,

there is a polynomial $f_{S_{1,r,1}} \in \mathbb{F}[X]$ taking values in (b_0, \dots, b_r) . The Newton interpolation formula defines $f_{S_{s,r,1}}$ by the following formula

$$(3.7) \quad f_{S_{1,r,1}}(X) := \lambda_0 + \lambda_1 X + \lambda_2 X(X-1) + \dots + \lambda_r X(X-1) \cdots (X-r),$$

where the coefficients $\lambda_k \in \mathbb{F}$ are defined inductively on k by solving the system of the following linear equations with coefficients in \mathbb{N}

$$\lambda_0 = b_0,$$

$$\lambda_0 + \lambda_1 = b_1,$$

$$\dots$$

$$(3.8) \quad \lambda_0 + \lambda_1 \cdot k + \dots + \lambda_k \cdot k! = b_k,$$

etc.

Next, let us assume that $s_0 \geq 2$ and Proposition 3.6 is valid for $s \leq s_0 - 1$. Now we show how to construct the required polynomial $f_{S_{s_0,r,1}}$. Recall that $f_{S_{s_0,r,1}} : \mathbb{F}^{s_0} \rightarrow \mathbb{F}$ is required to satisfy the following equation

$$(3.9) \quad f_{S_{s_0,r,1}}(i_1, i_2, \dots, i_{s_0}) = b_{i_1, \dots, i_{s_0}} \in S_{s_0,r,1} \subset \mathbb{F}$$

$$\text{for all } (i_1, \dots, i_{s_0}) \text{ such that } X_1^{i_1} \cdots X_s^{i_s} \in \text{Mon}_{s_0}^r.$$

We set

$$(3.10) \quad \begin{aligned} f_{S_{s_0,r,1}}(X_1, \dots, X_{s_0}) &:= P^r(X_1, \dots, X_{s_0-1}) + X_{s_0} P^{r-1}(X_1, \dots, X_{s_0-1}) + \dots \\ &+ X_{s_0}(X_{s_0} - 1) \cdots (X_{s_0} - r + 1) P^0(X_1, \dots, X_{s_0-1}). \end{aligned}$$

To determine the polynomials $P^k(X_1, \dots, X_{s_0-1})$ entered in (3.10) for $0 \leq k \leq r$ we exploit the following canonical injective map

$$(3.11) \quad \text{Mon}_{s-1}^r \rightarrow \text{Mon}_s^r, X_1^{i_1} \cdots X_{s-1}^{i_{s-1}} \mapsto X_1^{i_1} \cdots X_{s-1}^{i_{s-1}},$$

as well as the following canonical inclusions

$$(3.12) \quad \text{Mon}_{s-1}^r \supset \text{Mon}_{s-1}^{r-1} \supset \text{Mon}_{s-1}^{r-2} \supset \text{Mon}_{s-1}^{r-3} \supset \dots$$

Using (3.11) and (3.12) we denote the restriction of H_s^r to $\text{Mon}_{s_0-1}^{r-k}$ by $H_{s_0-1}^{r-k}$. The image $H_{s_0-1}^{r-k}(\text{Mon}_{s_0-1}^{r-k})$ is a set $S_{s_0-1,r-k}$ of $\binom{s_0-1+r-k}{r-k}$ elements in $\mathbb{F}^{s_0-1} \subset \mathbb{F}^{s_0}$. Clearly, for $0 \leq k \leq r$

$$S_{s_0-1,r-k} = \{(i_0, \dots, i_{s_0-1}, k) \mid i_j \in \mathbb{N} \text{ and } \sum_{j=1}^s i_j \leq r-k\} \subset S_{s_0,r}.$$

Next we decompose

$$S_{s_0,r,1} := \{b_{i_0, i_1, \dots, i_s} \mid i_j \in \mathbb{N} \text{ and } \sum_{j=1}^s i_j \leq r\} \subset \mathbb{F}$$

as a union of its disjoint subsets

$$S_{s_0,r,1} = S_{s_0-1,r,1} \cup S_{s_0-1,r-1,1} \cup \cdots \cup S_{s_0-1,0,1},$$

where for $0 \leq k \leq r$

$$S_{s_0-1,r-k,1} := \{b_{i_0,\dots,i_{s_0-1},k} \mid i_j \in \mathbb{N} \text{ and } \sum_{j=1}^s i_j \leq r-k\} \subset S_{s_0,r,1}.$$

Substituting $X_{s_0} = 0$ into (3.10), taking into account (3.9), we observe that the polynomial $P^r(X_1, \dots, X_{s_0-1})$ satisfies the following equation

$$(3.13) \quad P^r(i_1, \dots, i_{s_0-1}) = b_{i_0,\dots,i_{s_0-1},0} \in S_{s_0-1,r,1} \subset \mathbb{F}$$

for all (i_1, \dots, i_{s_0}) such that $(X_1^{i_1} \cdots X_{s_0-1}^{i_{s_0-1}}) \in \text{Mon}_{s_0-1}^r$.

The induction assumption implies that $P^r(X_0, \dots, X_{s_0-1})$ can be defined algorithmically such that (3.13) holds.

Now we will construct polynomials $P^{r-1}, P^{r-2}, \dots, P^0$ inductively from (3.9), (3.10) and (3.13). Assume this has been done for all P^r, \dots, P^{r-k+1} , $1 \leq k \leq r+1$. Substituting $X_{s_0} = k$ into (3.10) and comparing this with (3.9), we obtain the following defining equation for $P^{r-k} : \mathbb{F}^{s_0-1} \rightarrow \mathbb{F}$

$$(3.14) \quad f_{S_{s_0,r}}(i_1, \dots, i_{s_0-1}, k) = P^r(i_1, \dots, i_{s_0-1}) + kP^{r-1}(i_1, \dots, i_{s_0-1}) + \cdots + k!P^{r-k}(i_1, \dots, i_{s_0-1}) = b_{i_1,\dots,i_{s_0-1},k}.$$

$$(3.15) \quad \iff P^{r-k}(i_1, \dots, i_{s_0-1}) = b_{i_1,\dots,i_{s_0-1}}^{r-k} \in \mathbb{F}^m$$

for all (i_1, \dots, i_{s_0-1}) such that $(X_1^{i_1} \cdots X_{s_0-1}^{i_{s_0-1}}) \in \text{Mon}_{s_0-1}^r$ and for

$$b_{i_1,\dots,i_{s_0-1}}^{r-k} := \frac{1}{k!} [b_{i_1,\dots,i_{s_0-1},k} - (P^r(i_1, \dots, i_{s_0-1}) + kP^{r-1}(i_1, \dots, i_{s_0-1}) + \cdots + k!P^{r-k+1}(i_1, \dots, i_{s_0-1}))].$$

By the induction assumption P^{r-k} can be algorithmically constructed using (3.15). This completes the induction step. Hence Proposition 3.6 is valid for all s . \square

Corollary 3.7 (cf. Example 3.3). *Assume that $\{b_1, \dots, b_m\}$ are linearly independent vectors in \mathbb{F}^m . Then there exists a polynomial map $f : \mathbb{F} \rightarrow \mathbb{F}^m$ of degree m whose image contains the points $b_0 = 0, b_1, \dots, b_m$. In other words, f is $(m-1, 1)$ -elusive.*

Let us consider the interpolation problem for homogeneous polynomial mappings. Since each homogeneous polynomial $f \in \text{Pol}_{\text{hom}}^r(\mathbb{F}^{n+1}, \mathbb{F}^m) \subset \text{Pol}^r(\mathbb{F}^{n+1}, \mathbb{F}^m)$ is defined uniquely by the value of its restriction to

the hyperplane $b^{n+1} = 1$ in \mathbb{F}^{n+1} , we get immediately from Proposition 3.6

Corollary 3.8. 1. Given a tuple $S_{s,r,m}$ of $\binom{s+r}{r}$ points b_{i_1, \dots, i_s} in \mathbb{F}^m , $i_j \in \mathbb{N}$ and $\sum_{j=1}^s i_j \leq r$, there exists an algorithmically constructed homogeneous polynomial mapping $f_{S_{s,r,m}} : \mathbb{F}^{s+1} \rightarrow \mathbb{F}^m$ of degree r such that

$$(3.16) \quad f_{S_{s,r,m}}(i_1, \dots, i_s, 1) = b_{i_1, \dots, i_s}$$

for all (i_1, \dots, i_s) satisfying $i_j \in \mathbb{N}$ and $\sum_{j=1}^s i_j \leq r$.

2. Let us abbreviate $\binom{s+r}{r}$ by $b(s, r)$. Proposition 3.6 and the formulas in its proof give a linear isomorphism

$$(3.17) \quad I_m^{b(s,r)} : \mathbb{F}^{mb(s,r)} \rightarrow \text{Pol}^r(\mathbb{F}^s, \mathbb{F}^m),$$

which associates any point $\overline{S_{s,r,m}} \in \mathbb{F}^{mb(s,r)}$ with a polynomial mapping $f_{S_{s,r,m}} \in \text{Pol}^r(\mathbb{F}^s, \mathbb{F}^m)$.

Proposition 3.6 motivates the following

Definition 3.9. A mapping $f \in \text{Pol}^p(\mathbb{F}^n, \mathbb{F}^m)$ is called *strongly (s, r) -elusive*, if the set $\{f(i_1, \dots, i_n) \mid i_j \in \mathbb{N} \text{ and } \sum_{j=1}^n i_j \leq p\}$ is (s, r) -elusive.

Remark 3.10. 1. By Lemma 3.4, a polynomial mapping $f \in \text{Pol}^p(\mathbb{F}^n, \mathbb{F}^m)$ is strongly (s, r) -elusive, if and only if the point in $\mathbb{F}^{d(p,n,m)}$ associated with the tuple $(f(i_1, \dots, i_n) \mid i_j \in \mathbb{N} \text{ and } \sum_{j=1}^n i_j \leq p)$ belongs to the image of the evaluation mapping $Ev_{r,s,m}^{b(p,n)}$.

2. A strongly (s, r) -elusive polynomial mapping $f \in \text{Pol}^p(\mathbb{F}^n, \mathbb{F}^m)$ is (s, r, k) -elusive for any $k \geq \binom{n+p}{p}$, and, hence, it is (s, r) -elusive.

3. If $f \in \text{Pol}^p(\mathbb{F}^n, \mathbb{F}^m)$ is (strongly) (s, r) -elusive, then it is (strongly) (s', r) -elusive for any $s' \leq s$. If $f \in \text{Pol}^p(\mathbb{F}^n, \mathbb{F}^m)$ is not constant, then f is strongly $(0, r)$ -elusive for any r .

4. A polynomial mapping f is called *quasi-strongly (s, r) -elusive*, if there is an affine map $A \in \text{Aff}_{n,n}$ such that A^*f is strongly (s, r) -elusive. Using the argument below, we can show that the notion of quasi-strong (s, r) -elusiveness is defined by an polynomial type algebraic complexity.

Remark 3.10.3 motivates introducing a new polynomial type algebraic complexity. First we need some notations. Set

- $V_{s,r}^{p,n,m} := \text{Pol}^r(\mathbb{F}^s, \mathbb{F}^m) \times (\mathbb{F}^s)^{b(p,n)}$.
- $P_{s,r} : V_{s,r}^{p,n,m} \rightarrow \text{Pol}^p(\mathbb{F}^n, \mathbb{F}^m)$, $(g, y) \mapsto I_{m,n}^{b(p,n)} \circ Ev_{r,s,m}^{b(p,n)}(g, y)$,
where $g \in \text{Pol}^r(\mathbb{F}^s, \mathbb{F}^m)$ and $y \in (\mathbb{F}^s)^{b(p,n)}$.
- An element $(g, y) \in \text{Pol}^r(\mathbb{F}^s, \mathbb{F}^m) \times (\mathbb{F}^s)^{b(p,n)}$ is called a *computational model* for $f \in \text{Pol}^p(\mathbb{F}^n, \mathbb{F}^m)$, if $P_{s,r}(g, y) = f$.

- For $f \in \text{Pol}^p(\mathbb{F}, \mathbb{F}^m)$ denote

$$\mathcal{C}_r(f) := \bigcup_s \{(g, y) \in V_{(r,s)} \mid P_{r,s}(g, y) = f\}.$$

- Set $\mathcal{A} := \mathbb{N}$. Let $\Pi : V_{r,s} \rightarrow V_{r,s}$ be the identity mapping.
- Assume that p, n, m, r are given, and let $s \in \mathcal{A} = \mathbb{N}$. Then we check easily that $(V_s^r := V_{m-s,r}^{p,n,m}, K_p, \Pi, \hat{P}_s^r := P_{m-s,r})$ satisfy the condition in Definition 2.5.

For a non-constant polynomial mapping $f \in \text{Pol}^p(\mathbb{F}^n, \mathbb{F}^m)$ set

$$(3.18) \quad S_r(f) := \min\{s \mid f \in \hat{P}_s^r V_s^r\}.$$

Then $S_r(f)$ is a polynomial type algebraic complexity.

Definition 3.11. We call $S_r(f)$ the r -strong elusiveness of a non-constant polynomial mapping $f \in \text{Pol}^p(\mathbb{F}^n, \mathbb{F}^m)$.

The polynomial type algebraic complexity $S_r(f)$ suggests a new approach to study elusive functions, which we shall discuss in a separate note.

4. ZARISKI CLOSURE OF THE IMAGE OF A POLYNOMIAL MAPPING, EFFECTIVE ELIMINATION THEORY AND ALGEBRAIC NUMBER FIELD THEORY

In the previous sections we have seen that computation of a polynomial type algebraic complexity of a polynomial mapping $f \in \text{Pol}^p(\mathbb{F}^n, \mathbb{F}^m)$ (resp. verification of the strong (s, r) -elusiveness of a polynomial mapping f), can be reduced to the following problem. Given a polynomial map $\tilde{f} : \mathbb{F}^{N(p,n,m)} \rightarrow \mathbb{F}^{M(p,n,m)}$ and given a point $b \in \mathbb{F}^m$, verify whether b belongs to the image $\tilde{f}(\mathbb{F}^{N(p,n,m)})$. This problem is in fact a part of the elimination theory, which we discuss in this section (Lemma 4.1, Corollary 4.2). We develop the method invented by Kumar-Lokam-Patankar-Sarma [9] that uses effective elimination theory combined with algebraic number field theory in order to get concrete points b which do not belong to the Zariski closure of the image of a polynomial mapping \tilde{f} , if \tilde{f} is defined over \mathbb{Q} , such that the coordinates of b are algebraic numbers (Proposition 4.5). This result will be used in section 6 to find a sufficient condition for a polynomial mapping f to be strongly (s, r) -elusive.

Given a polynomial mapping $f \in \text{Pol}(\mathbb{F}^n, \mathbb{F}^{n+k})$, where $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$ and $k \geq 1$, we are interested in the image $f(\mathbb{F}^n) \subset \mathbb{F}^{n+k}$. For $\mathbb{F} = \mathbb{C}$, we will show in the next section an algorithm to detect whether a point b belongs to $f(\mathbb{F}^n)$. There are also several available methods

to detect whether a point b belongs to the Zariski closure $\overline{f(\mathbb{F}^n)}$ of $f(\mathbb{F}^n) \subset \mathbb{F}^{n+k}$, based on algebraic description of the ideal of the subvariety $\overline{f(\mathbb{F}^n)}$. The polynomial mapping $f = (f^1, \dots, f^{n+k})$ induces a ring homomorphism

$$f^* : \mathbb{F}[Y_1, \dots, Y_{n+k}] \rightarrow \mathbb{F}[X_1, \dots, X_n], \quad Y_i \mapsto f^i(X_1, \dots, X_n).$$

Denote by $I(f(\mathbb{F}^n))$ the ideal of $f(\mathbb{F}^n)$ (i.e. the ideal of all polynomials on \mathbb{F}^m which vanish on $f(\mathbb{F}^n)$).

Lemma 4.1. [3, Proposition 15.30], [6, Lemma 1.8.16] *Assume that f is a polynomial mapping from \mathbb{F}^n to \mathbb{F}^{n+k} . Then*

1. $\ker f^* = I(f(\mathbb{F}^n)) = I(\overline{f(\mathbb{F}^n)})$.
2. *Let I be the ideal in $\mathbb{F}[X_1, \dots, X_n, Y_1, \dots, Y_{n+k}]$ generated by $\{Y_1 - f^1, \dots, Y_{n+k} - f^{n+k}\}$. Then*

$$\ker f^* = I \cap \mathbb{F}[Y_1, \dots, Y_{n+k}].$$

Remark 4.2. Let $f : \mathbb{F}^n \rightarrow \mathbb{F}^m$ and $g : \mathbb{F}^s \rightarrow \mathbb{F}^m$ be two polynomial mappings. Clearly, $f(\mathbb{F}^n) \not\subset g(\mathbb{F}^s)$, if $\overline{f(\mathbb{F}^n)} \not\subset \overline{g(\mathbb{F}^s)}$, equivalently by Lemma 4.1, if $\ker f^* \not\subset \ker g^*$.

In general it is hard to find explicitly an element in $\ker f^*$. We know only an algorithm for determining the generators of $\ker f^* = I \cap \mathbb{F}[Y_1, \dots, Y_{n+k}]$ based on Gröbner's basis, which is resumed in Proposition 5.4 below, and two methods for determining a special element of $\ker f^*$ - the resultant of the corresponding system of polynomials, which we also explain in the next section. This algorithm is time-consuming, and it does not give us any partial knowledge of the generators of $\ker f^*$ at the first glance. In [9] Kumar, Lokam, Patankar and Sarma used effective elimination theory to get partial knowledge of an element in $\ker f^*$ and combining this knowledge with algebraic number field theory they obtained concrete matrices with high rigidity. Their method is applicable for finding concrete points in \mathbb{F}^{n+k} , which do not belong the Zariski closure $\overline{f(\mathbb{F}^n)}$ of a polynomial mapping f .

Lemma 4.3. [2, p.6 Theorem 4] *Let $I = \langle f^1, \dots, f^s \rangle$ be an ideal in the polynomial ring $\mathbb{F}[Y_1, \dots, Y_m]$ over an infinite field \mathbb{F} . Let d be the maximum total degree of the generators f^i . Let $Z = \{Y_{i_1}, \dots, Y_{i_s}\}$ be a subset of indeterminates $\{Y_1, \dots, Y_m\}$. If $I \cap \mathbb{F}[Z] \neq 0$ then there exists a non-zero polynomial $g \in I \cap \mathbb{F}[Z]$ such that $g = \sum_{i=1}^s g^i f^i$ with $g^i \in \mathbb{F}[Y_1, \dots, Y_m]$ and $\deg(g^i f^i) \leq (\mu + 1)(m + 2)(d^\mu + 1)^{\mu+2}$ for $i \in [1, s]$, where $\mu = \min\{s, m\}$.*

$$\text{Set } D(m, r) = (m + 1)(m + 2)(r^m + 1)^{m+2}.$$

Remark 4.4. Applying Lemmata 4.1 and 4.3 to the ideal $I = \langle Y_1 - f^1, \dots, Y_{n+k} - f^{n+k} \rangle$, and $Z = \mathbb{F}[Y_1, \dots, Y_{n+k}]$, observing that $I \cap \mathbb{F}[Z] \neq 0$ since $k \geq 1$, we obtain an upper estimate for the *minimal degree* $D(n+k, \deg f)$ of a polynomial $g \in \ker f^* = I \cap \mathbb{F}[Z]$ depending on the total degree $\deg f$ of the components f^i of f , assuming that $k \geq 1$. Thus, to prove that a point $b \in \mathbb{F}^{n+k}$ does not belong to the image $f(\mathbb{F}^n) \subset \mathbb{F}^{n+k}$ it suffices to show that $g(b) \neq 0$ for any $g \in \text{Pol}^{D(n+k, \deg f)}(\mathbb{F}^n)$.

To find such a point $b \in \mathbb{F}^{n+k}$ we use the algebraic number field theory, assuming $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$, and that f is defined over \mathbb{Q} , i.e., all polynomials f^i in question are defined over \mathbb{Q} . Assume that p_1, \dots, p_m are distinct prime numbers such that $p_i \geq D(m, r) + 2$ for all i . Set $b^i := e^{\frac{2\pi\sqrt{-1}}{p_i}}$. The following Proposition is a generalization of [9, Theorem 8].

Proposition 4.5. *Let $s \leq m - 1$ and $f : \mathbb{F}^s \rightarrow \mathbb{F}^m$ be a polynomial mapping over \mathbb{Q} of degree r .*

1. *Assume that p_1, \dots, p_{s+1} are distinct prime numbers such that $p_i \geq D(m, r) + 2$ for all i . Set*

$$b^i := e^{\frac{2\pi\sqrt{-1}}{p_i}} \text{ and } \tilde{b}^i := \sum_{j=1}^i a_j^i b^j,$$

where $a_j^i \in \mathbb{Q}$ and $a_i^i \neq 0$. Then $\tilde{b} = (\tilde{b}^1, \dots, \tilde{b}^{s+1}, a^{s+2}, \dots, a^m) \in \mathbb{C}^m$ does not belong to the image of f for $\mathbb{F} = \mathbb{C}$ and for any $(a^{s+1}, \dots, a^m) \in \mathbb{Q}^{m-s}$.

2. *Assume that p_1, \dots, p_{s+1} are distinct prime numbers such that $p_i \geq 2D(m, r) + 3$ for all i . Set*

$$b^i := e^{\frac{2\pi\sqrt{-1}}{p_i}} \text{ and } \tilde{b}^i := \sum_{j=1}^i a_j^i (b^j + \overline{b^j}),$$

where $a_j^i \in \mathbb{Q}$ and $a_i^i \neq 0$. Then $\tilde{b} = (\tilde{b}^1, \dots, \tilde{b}^{s+1}, a^{s+2}, \dots, a^m) \in \mathbb{R}^m$ does not belong to the image of f for $\mathbb{F} = \mathbb{R}$ and for any $(a^{s+1}, \dots, a^m) \in \mathbb{Q}^{m-s}$.

Proof. Clearly Proposition 4.5 follows from Lemmas 4.1, 4.3, Remark 4.4 and Proposition 4.6 below. \square

Proposition 4.6. *Assume that p_1, \dots, p_m are distinct prime numbers such that $p_i \geq D + 3$ for all i . Set $b^i := e^{\frac{2\pi\sqrt{-1}}{p_i}}$ and $\tilde{b}^i := \sum_{j=1}^i a_j^i b^j$, where $a_j^i \in \mathbb{Q}$ and $a_i^i \neq 0$.*

1. Then for all $g \in \text{Pol}^D(\mathbb{Q}^m) \subset \text{Pol}^D(\mathbb{C}^m)$ we have

$$g(\tilde{b}^1, \dots, \tilde{b}^m) \neq 0.$$

2. Then for all $g \in \text{Pol}^{\lfloor \frac{D+1}{2} \rfloor}(\mathbb{Q}^m) \subset \text{Pol}^{\lfloor \frac{D+1}{2} \rfloor}(\mathbb{R}^m)$ we have

$$g(\text{Re}(\tilde{b}^1), \dots, \text{Re}(\tilde{b}^m)) \neq 0,$$

where $\lfloor \frac{D+1}{2} \rfloor$ denotes the integral part of $\frac{D+1}{2}$, and $\text{Re}(a)$ denotes the real part of $a \in \mathbb{C}$.

Proof. 1. Let us prove Proposition 4.6.1 by induction on m . For $m = 1$ this is trivial, since $[\mathbb{Q}(\tilde{b}^1) : \mathbb{Q}] = p_1 - 1 \geq D + 1$.

Now suppose that the statement is true when the number of variables is strictly less than m . Assuming the opposite, i.e., the statement is not true for m , i.e. there exists $g \in \text{Pol}^D(\mathbb{Q}^m) \subset \text{Pol}^D(\mathbb{C}^m)$ such that

$$(4.1) \quad g(\tilde{b}^1, \dots, \tilde{b}^m) = 0.$$

Let us write

$$g(Y_1, \dots, Y_m) = \sum_{i=0}^d g_i(Y_1, \dots, Y_{m-1}) Y_m^{d-i},$$

where $g_i \in \mathbb{Q}[Y_1, \dots, Y_{m-1}]$, since g is defined over \mathbb{Q} . If g does not depend on Y_m , or equivalently $g_i = 0$ for $i \in [0, d-1]$, the induction assumption implies that the induction statement is also valid for m , since $g = g_d \in \text{Pol}^D(\mathbb{Q}^{m-1}) \subset \text{Pol}^D(\mathbb{C}^{m-1})$ satisfies

$$g(\tilde{b}^1, \dots, \tilde{b}^m) \neq 0.$$

Thus, we can assume that Y_m enters in g . Hence

$$g(\tilde{b}^1, \dots, \tilde{b}^{m-1})(x) \neq 0 \in \mathbb{Q}(\tilde{b}^1, \dots, \tilde{b}^{m-1})[x].$$

Clearly, (4.1) implies that \tilde{b}^m satisfies a non-zero equation over $\mathbb{Q}(\tilde{b}^1, \dots, \tilde{b}^{m-1})$. Thus

$$(4.2) \quad [\mathbb{Q}(\tilde{b}^1, \dots, \tilde{b}^m) : \mathbb{Q}(\tilde{b}^1, \dots, \tilde{b}^{m-1})] \leq D.$$

Since $\tilde{b}^i = \sum_{j=1}^i a_j^i b^j$, where $a_j^i \in \mathbb{Q}$ and $a_i^i \neq 0$, we get easily

$$\mathbb{Q}(\tilde{b}^1, \dots, \tilde{b}^k) = \mathbb{Q}(b^1, \dots, b^k) \text{ for all } k \leq m.$$

Thus (4.3) implies that

$$(4.3) \quad [\mathbb{Q}(b^1, \dots, b^m) : \mathbb{Q}(b^1, \dots, b^{m-1})] \leq D.$$

Since $\mathbb{Q}(b^m)$ is a Galois extension of \mathbb{Q} , applying [10, Theorem 1.12 p. 266] we obtain

$$(4.4) \quad [\mathbb{Q}(b^1, \dots, b^m) : \mathbb{Q}(b^1, \dots, b^{m-1})] = [\mathbb{Q}(b^m) : \mathbb{Q}] = p_m - 1 \geq D + 1.$$

Thus, (4.3) does not hold. Hence Proposition 4.6.1 is also valid for m . This completes the proof of Proposition 4.6.1.

2. Now let us prove Proposition 4.6.2. Repeating the argument in the proof of Proposition 4.6.1 we derive Proposition 4.6.2 from the following

Lemma 4.7. *For $1 \leq i \leq m$, $\mathbb{Q}(Re(\tilde{b}^i))$ is a Galois extension of \mathbb{Q} and $[\mathbb{Q}(Re(\tilde{b}^i)) : \mathbb{Q}] \geq \lfloor \frac{D+1}{2} \rfloor$.*

Proof. Since $\mathbb{Q}(Re(\tilde{b}^i))$ is a subfield of the Galois extension $\mathbb{Q}(b^i)$, whose Galois group is cyclic, $\mathbb{Q}(Re(\tilde{b}^i))$ is also a Galois extension. Note that the Galois group $G_{\mathbb{Q}(Re(\tilde{b}^i))}$ of $\mathbb{Q}(Re(\tilde{b}^i))$ is $\mathbb{Z}_{p_i-1}/\mathbb{Z}_2$. Hence

$$[\mathbb{Q}(Re(\tilde{b}^i)) : \mathbb{Q}] \geq \#(G_{\mathbb{Q}(Re(\tilde{b}^i))}) = \frac{p_i - 1}{2} \geq \lfloor \frac{D+1}{2} \rfloor.$$

This proves Lemma 4.7. □

This completes the proof of Proposition 4.6. □

Remark 4.8. 1. Let $f : \mathbb{F}^n \rightarrow \mathbb{F}^m$ be a mapping. The question whether f is a polynomial mapping defined over \mathbb{Q} depends on the choice of a basis (V_1, \dots, V_n) of \mathbb{F}^n as well as on the choice of a basis (W_1, \dots, W_m) of \mathbb{F}^m . Assume that $f : \mathbb{F}^n \rightarrow \mathbb{F}^m$ is a polynomial mapping defined over \mathbb{Q} with respect to a basis (V_1, \dots, V_n) of \mathbb{F}^n and a basis (W_1, \dots, W_m) of \mathbb{F}^m . Then f is also a polynomial mapping defined over \mathbb{Q} with respect a basis (V'_1, \dots, V'_n) of \mathbb{F}^n and a basis (W'_1, \dots, W'_m) of \mathbb{F}^m , if $V'_i = \sum_j A_{ij} V_j$, $W'_i = \sum_l B_{il} W_l$ and A_{ij}, B_{il} are rational numbers. In other words, the basis (V'_i) (resp. (W'_j)) is obtained from the basis (V_i) (resp. (W_j)) by a linear transformation over \mathbb{Q} .

2. The set of all transformations $(a_j^i) \in Mat_n(\mathbb{Q})$ with $a_j^i = 0$ if $j > i$ and $a_i^i \neq 0$, which enter in Proposition 4.5, forms the solvable group $B_n(\mathbb{Q})$.

5. ALGORITHMS TO COMPUTE AND TO ESTIMATE POLYNOMIAL TYPE ALGEBRAIC COMPLEXITIES

In this section we present some nice properties of polynomial type algebraic complexities. First, we prove the following

Theorem 5.1. *Suppose that $f \in Pol(\mathbb{C}^n, \mathbb{C}^m)$ and $\mathcal{C}(f)$ is a class of computational models for f . Let $C_S(f)$ be a polynomial type computational complexity. There exists an algorithm to compute $C_S(f)$.*

The proof of Theorem 5.1 is based on Formula (2.11) relating $C_S(f)$ with the image of a polynomial mapping \hat{P}_α , which leads to an elimination problem by Lemma 4.1. In the remaining part of this section

we will describe an algorithm based on Gröbner's basis to solve this elimination problem, namely to determine the generators of $\ker f^* = I \cap \mathbb{F}[Y_1, \dots, Y_{n+k}]$ (Proposition 5.4). We also present two methods for determining a special element of $\ker f^*$, namely the resultant of the corresponding system of polynomials (Proposition 5.5, Remark 5.6). Note that any element of $\ker f^*$, in particular the resultant, is a test function for deciding whether a given point Y belongs to the Zariski closure $\overline{f(\mathbb{F}^n)} \subset \mathbb{F}^{n+k}$. By (2.11) a polynomial type algebraic complexity $C_S(f)$ is greater than $\alpha \in \mathbb{N}$ if and only if f does not belong to the image of the polynomial mapping \widehat{P}_α . Thus any element in $\ker(\widehat{P}_\alpha)^*$ is a test function for deciding if $C_S(f) \geq \alpha$.

Proof of Theorem 5.1. Recall that

$$C_S(f) = \min\{\alpha \mid f \in \widehat{P}_\alpha(V_\alpha)\},$$

where $\alpha \in \mathcal{A} \subset \mathbb{N}$. To determine $C_S(f)$ it suffices to describe an algorithm for deciding whether $f \in \widehat{P}_\alpha(V_\alpha) \subset \text{Pol}(\mathbb{F}^n, \mathbb{F}^m)$, for each $\alpha \in \mathcal{A}$. Since \widehat{P}_α is a polynomial mapping, the function $K : \mathcal{A} \rightarrow \mathbb{N}$ is computable. As before we set $d(K(\alpha), n, m) := \dim \text{Pol}^{K(\alpha)}(\mathbb{F}^n, \mathbb{F}^m)$. We have to decide whether the following system of polynomial equations

$$\widehat{P}_\alpha^i(a) = f^i, \quad i \in [1, d(K(\alpha), n, m)],$$

has a solution $a \in V_\alpha$. Here \widehat{P}_α^i is the i -th component of the polynomial mapping $\widehat{P}_\alpha : V_\alpha \rightarrow \text{Pol}^{K(\alpha)}(\mathbb{F}^n, \mathbb{F}^m)$, and f^i is the i -th coordinate of $f \in \text{Pol}^{K(\alpha)}(\mathbb{F}^n, \mathbb{F}^m)$.

This problem has been solved, see e.g., [6, §1.8.4]. The solution is based on Hilbert's Nullstellensatz, which implies that a system of polynomial equations $\{f_i = b_i \in \mathbb{C}; i \in [1, d]\}$ has no solution, if and only if 1 belongs to the ideal generated by $\{f_i - b_i, i = \overline{1, d}\}$.

Lemma 5.2. [6, §1.8.4] *Let I be an ideal in $\mathbb{C}[X_1, \dots, X_n]$ generated by $\{f_i - b_i; i \in [1, d]\}$, $f_i \in \mathbb{C}[X_1, \dots, X_n]$, $b_i \in \mathbb{C}$, and G a Gröbner basis of I . Then the system of polynomial equations $\{f_i = b_i; i \in [1, d]\}$ has a solution, if and only if G contains no element of degree 0.*

This completes the proof of Theorem 5.1. □

Corollary 5.3. *There exists an algorithm based on Gröbner bases to compute the determinantal complexity of any polynomial f over \mathbb{C} .*

Now we explain a method of computing the Gröbner basis of $\ker f^*$. For any ordering on $\mathbb{F}[X_1, \dots, X_n, Y_1, \dots, Y_{n+k}]$ denote by $LM(f)$ the leading monomial of f with respect to that ordering. An ordering is

called an *elimination ordering with respect to the initial subset* (X_1, \dots, X_n) of variables if

$$\begin{aligned} f \in \mathbb{F}[X_i, \dots, X_n, Y_1, \dots, Y_{n+k}], LM(f) \in \mathbb{F}[Y_1, \dots, Y_{n+k}] &\implies \\ \implies f \in \mathbb{F}[Y_1, \dots, Y_{n+k}]. \end{aligned}$$

For example, the lexicographical ordering is an elimination ordering with respect to every initial subset of variables.

Proposition 5.4. [3, Proposition 15.29], [6, Lemma 1.8.3] *Let $>$ be an elimination ordering with respect to (X_1, \dots, X_n) on $\mathbb{F}[X_1, \dots, X_n, Y_1, \dots, Y_{n+k}]$, and $I \subset \mathbb{F}[X_1, \dots, X_n, Y_1, \dots, Y_{n+k}]$ an ideal. If $S = \{g_1, \dots, g_{n+k}\}$ is a Gröbner basis of I and g_1, \dots, g_u are those g_i that do not involve the variables X_i , then g_1, \dots, g_u form a Gröbner basis for $I \cap \mathbb{F}[Y_1, \dots, Y_{n+k}]$.*

Using the resultant of polynomials in many variables, let us present another method to construct a test function T for a polynomial type algebraic complexity $C_S(f)$, $f \in \text{Pol}(\mathbb{F}^n, \mathbb{F}^n)$. This method goes back to Cayley and Poisson, see [5] for comments and a reprint of Cayley's result. We refer the reader to [8] and [10, §4 chapter IX] for a modern exposition of elimination theory using resultants. Recall that the resultant $R(f_1, \dots, f_{n+1})$ for a $(n+1)$ -tuple $f = (f_1, \dots, f_{n+1})$ of polynomial $f_i \in \mathbb{F}[X_1, \dots, X_n]$ is a polynomial in coefficients of f_i with the following property: $R(f_1, \dots, f_{n+1}) = 0$ if and only if f_1, \dots, f_{n+1} has a common zero $(a_1, \dots, a_n) \in (\mathbb{F})^n$, where \mathbb{F} is the algebraic closure of \mathbb{F} ; see [5, chapter 13] for more details. In particular, for any $(a_1, \dots, a_n) \in \mathbb{F}^n$ we have

$$(5.1) \quad R(f_1 - f_1(a_1, \dots, a_n), \dots, f_{n+1} - f_{n+1}(a_1, \dots, a_n)) = 0.$$

For a $(n+1)$ -tuple $f = (f_1, \dots, f_{n+1})$ we denote by $R_f(b_1, \dots, b_{n+1})$ the resultant $R(f_1 - b_1, \dots, f_{n+1} - b_{n+1})$, which is regarded as the value of polynomial $R_f(Y_1, \dots, Y_{n+1}) := R(f_1 - Y_1, \dots, f_{n+1} - Y_{n+1})$ in variables Y_1, \dots, Y_{n+1} at the point $(b_1, \dots, b_{n+1}) \in \mathbb{F}^{n+1}$. From (5.1) we get immediately

Proposition 5.5. *The resultant $R_f(Y_1, \dots, Y_{n+1}) \in \mathbb{F}[Y_1, \dots, Y_{n+1}]$ is a test function for the image of the polynomial mapping f in the sense that, if $R_f(a_1, \dots, a_{n+1}) \neq 0$ for some point $(a_1, \dots, a_{n+1}) \in \mathbb{F}^{n+1}$, then $(a_1, \dots, a_{n+1}) \in \mathbb{F}^m$ does not belong to the image of f .*

Remark 5.6. 1. Proposition 5.5 and (2.11) imply that the resultant $R_{\hat{P}_\alpha}$ is a test function for estimating the polynomial type algebraic complexity $C_S(f)$ defined by \hat{P}_α .

2. There are two methods to compute $R_f(Y_1, \dots, Y_{n+1})$, where $f = (f_1, \dots, f_{n+1})$ and $f_i \in \mathbb{F}[X_1, \dots, X_n]$. The first method consists in finding the determinant of an associated resultant complex [5, Theorem 1.4, chapter 13]. (The method presented in [5] is applicable only to homogeneous polynomial mappings $f = (f_1, \dots, f_{n+1}) \in \text{Pol}(\mathbb{F}^{n+1}, \mathbb{F}^{n+1})$). To extend this method to general polynomial mappings $f = (f_1, \dots, f_{n+1}) \in \text{Pol}(\mathbb{F}^n, \mathbb{F}^{n+1})$, we consider its homogenization $\tilde{f} = (\tilde{f}_1, \dots, \tilde{f}_{n+1}) \in \text{Pol}_{\text{hom}}(\mathbb{F}^{n+1}, \mathbb{F}^{n+1})$ such that $\tilde{f}(x, 1) = f(x)$ for all $x \in \mathbb{F}^n$. The second method consists in finding GCD of certain polynomials [5, Theorem 1.5, chapter 13].

3. Given a $(n+k)$ -tuple $f = (f_1, \dots, f_{n+k})$, $k \geq 1$, of polynomials $f_i \in \mathbb{F}[X_1, \dots, X_n]$, we denote by \tilde{f}_{n+1} the $(n+1)$ -tuple (f_1, \dots, f_{n+1}) . Lemma 4.1.1 implies that the resultant $R_{\tilde{f}_{n+1}}(Y_1, \dots, Y_{n+1})$, regarded as an element in $\mathbb{F}[Y_1, \dots, Y_{n+1}, \dots, Y_{n+k}]$, is also an element in $\ker f^*$.

4. Using similar ideas, we construct an algorithm for deciding whether a polynomial mapping $f \in \text{Pol}(\mathbb{F}^n, \mathbb{F}^m)$ is (s, r, k) -elusive. By Corollary 3.5 and Remark 4.2, it suffices to find an algorithm that verifies whether generators of $\ker(\text{Ev}_{s,r,m}^k)^*$ also belong to $\ker(\hat{f}^k)^*$. Such an algorithm is known, see e.g., [6, §1.8.11].

6. EXAMPLES AND APPLICATIONS

In this section, using the methods developed in the previous sections, we construct concrete examples of polynomials of large determinantal complexity (Example 6.2) and concrete examples of (s, r) -elusive functions (Proposition 6.6, Proposition 6.7). As a results, we construct a sequence of polynomials of large circuit size (Proposition 6.9).

To apply the effective elimination theory and the method developed in section 4 we need the following

Lemma 6.1. 1. For all $n, m \in \mathbb{N}$ the polynomial map $\mathcal{D}_{n,m} : \text{Aff}_{n,m^2} \rightarrow \text{Pol}^m(\mathbb{F}^n)$ is of degree m ; moreover it is defined over \mathbb{Q} .
 2. The evaluation map $\text{Ev}_{r,s,m}^k$, defined in (3.1), is of total degree $r+1$, it is also defined over \mathbb{Q} .

Proof. 1. The first assertion of Lemma 6.1 is trivial, so we omit its proof.

2. Let us compute the degree of the evaluation map $\text{Ev}_{r,s,m}^k$. Let $\{V_j, 1 \leq j \leq s\}$ be a basis of \mathbb{F}^s . For $1 \leq l \leq m$ let $\{(X_1^{i_1} \cdots X_s^{i_s})_l \mid \sum_{j=1}^s i_j \leq r\}$ be the basis consisting of monomials in $\text{Pol}^r(\mathbb{F}^s)$. Let $f = (f^1, \dots, f^m) \in \text{Pol}^r(\mathbb{F}^s, \mathbb{F}^m)$ where

$$f^l := \sum_{0 \leq i_1 + \dots + i_s \leq r} a_{i_1 \dots i_s, l} (X_1^{i_1} \cdots X_s^{i_s})_l.$$

Let $b = (b_1, \dots, b_k) \in (\mathbb{F}^s)^k$ where

$$b_i = \sum_j b_i^j V_j \in \mathbb{F}^s.$$

Then

$$(6.1) \quad Ev_{r,s,m}^k(f, b) = (f(\sum_{j=1}^s b_1^j V_j), \dots, f(\sum_{j=1}^s b_k^j V_j)) \in (\mathbb{F}^m)^k.$$

Clearly $Ev_{r,s,m}^k$ is a polynomial mapping, whose degree does not depend on k or on m . Note that for $k = 1$ and $m = 1$ we have

$$(6.2) \quad Ev_{r,s,1}^1(f, b) = \sum_{0 \leq i_1 + \dots + i_s \leq r} a_{i_1 \dots i_s} (b_1^1)^{i_1} \dots (b_1^s)^{i_s} \in \mathbb{F}.$$

(6.2) implies that $Ev_{r,s,1}^1$ is of degree 1 on f and of maximal degree r on b . This proves the second assertion of Lemma 6.1. \square

Using Lemma 6.1 we will construct concrete polynomials of large determinantal complexity in the following

Example 6.2. Assume that m, n, r are positive integers such that

$$\binom{r+n}{n} - 1 \geq (n+1)m^2.$$

1. Let $\{p_i, 1 \leq i \leq (n+1)m^2\}$ be distinct prime numbers such that for all i

(6.3)

$$p_i > D((n+1)m^2, m) = ((n+1)m^2+1)((n+1)m^2+2)(m^{(n+1)m^2}+1)^{(n+1)m^2+2}.$$

Let $\tilde{b}^i, i \in [1, \binom{n+r}{r}]$, be defined as in Proposition 4.5.1. Denote by $\lambda : \mathbb{N}^n \rightarrow \mathbb{N}$ the mapping defined by the lexicographical ordering. Let $f_n \in \text{Pol}^r(\mathbb{C}^n)$ be the polynomial whose coefficients $a_{i_1 \dots i_n}$ for monomial $X_1^{i_1} \dots X_n^{i_n} \in \text{Pol}^r(\mathbb{C}^n)$ are $\tilde{b}^{\lambda(i_1, \dots, i_n)}$. Lemma 6.1 and Proposition 4.5.1 imply that $c_{\det}(f_n) \geq m+1$.

2. In the same way, using Proposition 4.5.2 we find a concrete polynomial $f'_n \in \text{Pol}^r(\mathbb{R}^n)$, whose determinantal complexity is greater or equal to $m+1$.

Note that the sequence f_n (resp. f'_n) in Example 6.1 is not poly(n)-definable, if m is allowed to grow faster than polynomial of n . Later in this section, using elusive functions, we will construct explicit (poly(n)-definable) sequences of polynomials with large circuit size. First, we need

Definition 6.3. A polynomial $(X - i_1)(X - i_1 + 1) \cdots X \in \mathbb{F}[X]$ is called a *pseudo-monomial*, if $i_j \in \mathbb{N}$. A constant is also called a pseudo-monomial. A polynomial $f \in \mathbb{F}[X_1, \dots, X_n]$ is called a *pseudo-monomial*, if $f = f^1 \cdots f^n$, where, for $1 \leq i \leq n$, $f^i \in \mathbb{F}[X_i]$ and f^i is a pseudo-monomial.

Remark 6.4. 1. According to the lexicographical ordering in $Pol^r(\mathbb{F}^n, \mathbb{F}^m)$ the linear transformation $Pol^p(\mathbb{F}^n, \mathbb{F}^m) \rightarrow Pol^p(\mathbb{F}^n, \mathbb{F}^m)$ sending the basis consisting of pseudo-monomials to the standard basis of monomials is an element of the solvable group $B_{m \binom{n+p}{p}}(\mathbb{Q})$. In particular, any polynomial $f \in Pol^p(\mathbb{F}^n, \mathbb{F}^m)$ can be written in a unique way as a linear combination of pseudo-monomials.

2. The notion of pseudo-monomials is motivated by the interpolation formulas (3.7), (3.8), (3.9), (3.15), (3.16) for polynomial mappings. Using these formulas we have defined the coefficients $\lambda_{i_1, \dots, i_n}^i$ of the pseudo-monomials $(X_1 - i_1)(X_1 - i_1 + 1) \cdots X_1(X_2 - i_2) \cdots X_2 \cdots (X_n - i_n) \cdots X_n$ in the component f^i of a polynomial mapping $f : \mathbb{F}^n \rightarrow \mathbb{F}^m$ as a rational linear combination of the coordinates of the given points $b_{i_1 \dots i_n} \in \mathbb{F}^m$.

Next, we need the following

Lemma 6.5. Assume that $1 \leq s < m$. Then there exists a (s, r) -elusive K -tuple in \mathbb{F}^m , if

$$(6.4) \quad K \geq \frac{m \binom{s+r}{s} + 1}{m - s}.$$

Proof. Note that

$$\dim(Pol^r(\mathbb{F}^s, \mathbb{F}^m) \times (\mathbb{F}^s)^K) = m \binom{s+r}{s} + sK.$$

It follows that the image of the evaluation map $Ev_{s,r,m}^K$ is a proper subset of co-dimension at least 1 in \mathbb{F}^{mK} if K satisfies (6.4). Taking into account Lemma 3.4, we obtain immediately Lemma 6.5. \square

Using the interpolation formula we shall construct from (s, r) -elusive K -tuples in \mathbb{F}^m (s, r) -elusive polynomial mappings $f : \mathbb{F}^n \rightarrow \mathbb{F}^m$. Given K satisfying (6.4), let us assume that two positive integers n, p satisfy the following conditions

$$(6.5) \quad \binom{n+p}{n} \geq K \geq \frac{m \binom{s+r}{s} + 1}{m - s}.$$

By Proposition 3.6, the first inequality in (6.5) is a sufficient condition for the existence of a polynomial mapping $f \in Pol^p(\mathbb{F}^n, \mathbb{F}^m)$ such that the image $f(\mathbb{F}^n)$ contains a given K -tuple in \mathbb{F}^m .

Proposition 6.6. *Assume that n, p satisfy (6.5) with $K = \binom{n+p}{n}$.*

1. *Assume that f^1, \dots, f^m are polynomials in $\text{Pol}^p(\mathbb{C}^n)$ such that the monomial (resp. pseudo-monomial) coefficients of each f^j , according to the lexicographical ordering, and beginning with the smallest term, are*

$$e^{\frac{2\pi\sqrt{-1}}{p_1^j}}, \dots, e^{\frac{2\pi\sqrt{-1}}{p_K^j}}$$

where $\{p_i^j, 1 \leq i \leq K, 1 \leq j \leq m\}$ are distinct prime numbers such that $p_i^j \geq D(m, r) + 2$. Then the polynomial mapping $f = (f^1, \dots, f^m) : \mathbb{C}^n \rightarrow \mathbb{C}^m$ is (s, r) -elusive.

2. *Assume that f^1, \dots, f^m are polynomials in $\text{Pol}^p(\mathbb{R}^n)$ such that the monomial (resp. pseudo-monomial) coefficients of each f^j , according to the lexicographical ordering, and beginning with the smallest term, are*

$$\text{Re}(e^{\frac{2\pi\sqrt{-1}}{p_1^j}}), \dots, \text{Re}(e^{\frac{2\pi\sqrt{-1}}{p_K^j}}),$$

where $\{p_i^j, 1 \leq i \leq K, 1 \leq j \leq m\}$ are distinct prime numbers such that $p_i^j \geq 2D(m, r) + 3$. Then the polynomial mapping $f = (f^1, \dots, f^m) : \mathbb{R}^n \rightarrow \mathbb{R}^m$ is (s, r) -elusive.

Proof. It suffices to show that the polynomial mappings f defined in Proposition 6.6 are strongly (s, r) -elusive. Equivalently, we need to show that the set

$$S_K := \{f(i_1, \dots, i_n) \mid i_j \in \mathbb{N} \text{ and } \sum_{j=1}^n \leq p\} \subset \mathbb{F}^m,$$

$\mathbb{F} = \mathbb{C}$ or $\mathbb{F} = \mathbb{R}$, is a (s, r) -elusive K -tuple. We will show that the associated point $\overline{S_K} \in (\mathbb{F}^m)^K$ does not belong to the image of the evaluation map $Ev_{r,s,m}^K$. By Lemma 6.1 the evaluation map $Ev_{r,s,m}^K$ is a polynomial mapping of degree $(r+1)$, moreover it is defined over \mathbb{Q} . Remarks 4.8 and 6.4.2 imply that Lemma 6.1 also holds with respect to the basis of $(\mathbb{F}^m)^K = (\mathbb{F}^K)^m = \text{Pol}^r(\mathbb{F}^n, \mathbb{F}^m)$ that is induced from the basis of pseudo-monomials in $\text{Pol}^r(\mathbb{F}^n)$. Now we will apply Proposition 4.5 to show that $\overline{S_K}$ is a regular value of $Ev_{r,s,m}^k$; more precisely, we will verify that the coordinates of $\overline{S_K}$ with respect to the pseudo-monomial basis in $(\mathbb{F}^K)^m = \text{Pol}^r(\mathbb{F}^n, \mathbb{F}^m)$ satisfy the conditions of Proposition 4.5. Using Remarks 4.8.2 and 6.4.1 it suffices to consider the case of $f \in \text{Pol}^p(\mathbb{F}^n, \mathbb{F}^m)$ with pseudo-monomial coefficients being the given numbers.

By the assumption of Proposition 6.6 the first m coordinates of $\overline{S_K} \in (\mathbb{F}^K)^m = \text{Pol}^r(\mathbb{F}^n, \mathbb{F}^m)$ are the smallest pseudo-monomials according to

the lexicographical ordering, i.e., they are field elements. These field elements are numbers

$$e^{\frac{2\pi\sqrt{-1}}{p_1^1}} \dots, e^{\frac{2\pi\sqrt{-1}}{p_1^m}},$$

if $\mathbb{F} = \mathbb{C}$. (The case $\mathbb{F} = \mathbb{R}$ is similar). Now assume that the conditions of Proposition 4.5 hold for the first lm -coordinates of $\overline{S_K} \in (\mathbb{F}^K)^m = \text{Pol}^r(\mathbb{F}^n, \mathbb{F}^m)$, for $l \geq 1$. The interpolation formula (3.15) for the $(l+1)j$ coordinate $(S_K)_{l+1}^j$ of $\overline{S_K}$, $1 \leq j \leq m$, if $\mathbb{F} = \mathbb{C}$, has the following form

$$(\overline{S_K})_j^{l+1} = a_j^{l+1} e^{\frac{2\pi\sqrt{-1}}{p_{l+1}^j}} + \sum_{1 \leq k \leq l} a_j^{l+1,k} e^{\frac{2\pi\sqrt{-1}}{p_k^j}},$$

where $a_j^{l+1,k} \in \mathbb{Q}$ and $a_j^{l+1} \neq 0$. (The case $\mathbb{F} = \mathbb{R}$ is similar). Thus the conditions in Proposition 4.5 also hold for first $(l+1)m$ -coordinates of $\overline{S_K} \in (\mathbb{F}^K)^m = \text{Pol}^r(\mathbb{F}^n, \mathbb{F}^m)$. This completes the proof of Proposition 6.6. \square

Proposition 6.7. *Given $4 \leq r' \in \mathbb{N}$, for $n \in \mathbb{N}$ set*

$$s(n) := (\lfloor \frac{n}{(r'-1)r'} \rfloor)^{r'-3}, \quad m(n) := n \cdot \binom{n-1+r'}{r'}, \quad p = (r'-1)(2r'-1).$$

Then, for $\mathbb{F} = \mathbb{C}$ or $\mathbb{F} = \mathbb{R}$, there exists a $\text{poly}(n)$ -definable polynomial mapping $f \in \text{Pol}^p(\mathbb{F}^n, \mathbb{F}^{m(n)})$ such that f is $(s(n), 2r'-1)$ -elusive.

Proof. Set $r := 2r' - 1$. Let $n = (r' - 1)n'$, where $n' \in \mathbb{N}$ such that $(n+r-4)^4 \geq r!$. We will show that (n, p, m, s, r) defined in Proposition 6.7 satisfy (6.5) for $K := \binom{n+p}{p}$, i.e., we need to verify that

$$(6.6) \quad \binom{n+p}{n} \geq \frac{m \binom{s+r}{s} + 1}{m-s}.$$

Since $(n+r-4)^4 \geq r!$ we get

$$(6.7) \quad s(n) \leq n^{r'-3} \leq \frac{n}{2} n^{r'-4} \leq \frac{n}{2} \cdot \binom{n-1+r'}{r'} \leq \frac{m+1}{2}.$$

It follows that

$$(6.8) \quad \frac{m \binom{s+r}{s} + 1}{m-s} \leq \frac{(m+1) \binom{s+r}{s}}{m-s} \leq \frac{(m+1) \binom{s+r}{s}}{m - \frac{m+1}{2}} \leq 2 \left(1 + \frac{2}{m-1}\right) \binom{s+r}{s}.$$

Clearly (6.6) follows from (6.8) and the following inequality

$$(6.9) \quad \binom{n+p}{n} \geq 2 \left(1 + \frac{2}{m-1}\right) \binom{s+r}{s},$$

which we now prove. We rewrite the LHS of (6.9) as

$$(6.10) \quad \prod_{k=0}^{r-1} \frac{(n + (r' - 1)k + 1)(n + (r' - 1)k + 2) \cdots (n + (r' - 1)(k + 1))}{((r' - 1)k + 1)((r' - 1)k + 2) \cdots (r' - 1)(k + 1)}.$$

We rewrite the RHS of (6.9) as

$$(6.11) \quad 2(1 + \frac{2}{m-1}) \prod_{k=1}^r \frac{s+k}{k}.$$

Using (6.10) and (6.11) we deduce (6.9) from the following obvious inequality

$$(6.12) \quad \frac{(n')^{r'-1}}{(k+1)^{r'-1}} \geq \frac{s+k+1}{k+1} + 1 \text{ for all } 0 \leq k \leq r-1.$$

Thus we can apply Proposition 6.6 to get a (s, r) -elusive mapping $f \in \text{Pol}^p(\mathbb{F}^n, \mathbb{F}^m)$, whose monomial coefficients are p_j^i in Proposition 6.6.

Note that the dimension of the space $\text{Pol}^p(\mathbb{C}^n, \mathbb{C}^m)$ is $m \binom{n+p}{p} \leq (2n)^{r'+1+p}$, if $n \geq p > r' + 1$. Write $f = (f^1, \dots, f^m) \in \text{Pol}^p(\mathbb{F}^n, \mathbb{F}^m)$. By construction each monomial coefficient of f^i is given. Since p is constant, f is $\text{poly}(n)$ -computable, and hence $\text{poly}(n)$ -definable. This completes the proof of Proposition 6.7. \square

In [13, §3.4] Raz proposed a method for constructing polynomials of large complexity using (s, r) -elusive functions. Propositions 6.8, 6.9 below are sample applications of Raz's method.

Given a tuple of n^2 function $f_{ij} \in \mathbb{F}[X_1, \dots, X_n]$, $1 \leq i, j \leq n$, we define an n -tuple of polynomials $\tilde{f}_i \in \mathbb{F}[X_1, \dots, X_n, Z_1, \dots, Z_n]$, $i \in [1, n]$, as follows (cf. [13, §3.3])

$$(6.13) \quad \tilde{f}_i(X_1, \dots, X_n, Z_1, \dots, Z_n) := \sum_{j=1}^n f_{ji}(X_1, \dots, X_n) Z_j$$

Proposition 6.8. [13, Proposition 3.11] *Let $n, r \leq s$ be integers. Let $f : \mathbb{F}^n \rightarrow \mathbb{F}^{n^2}$ be a polynomial mapping. If f is (s, r) -elusive, then any depth- r arithmetic circuit over \mathbb{F} for the n -tuple $\{\tilde{f}_i : \mathbb{F}^{2n} \rightarrow \mathbb{F}, i \in [1, n]\}$ of polynomials defined by (6.13) is of size greater than s .*

Using Proposition 6.8 and our construction of (s, r) -elusive functions in Proposition 6.6, taking into account Proposition 5.1 and Proposition 6.5 we shall construct sequences of polynomials with large circuit size.

Proposition 6.9. *Let $\mathbb{F} = \mathbb{C}$ or $\mathbb{F} = \mathbb{R}$, and $1 \leq r \in \mathbb{N}$. There are infinitely many sequences of $\text{poly}(n)$ -definable polynomials $\tilde{f}_{n,r} \in$*

$Pol^{5r+1}(\mathbb{F}^{2n}, \mathbb{F}^n)$, which satisfy the following properties. All the coefficients of $\tilde{f}_{n,r}$ are algebraic numbers, and any depth- r arithmetic circuit over \mathbb{F} for $\tilde{f}_{n,r}$ is of size greater than $\frac{n^2}{50r^2}$.

Proof. Let $n' \geq r^2$ be an integer, and set

$$n := 5n'r, p := 5r, m := (n')^2, s := \lfloor (n')^2/2 \rfloor.$$

First we will show that the chosen values (n, p, m, s) satisfy Condition (6.5). Since $(m - s) \geq m/2$ it suffices to show

$$(6.14) \quad \binom{5n'r + 5r}{5r} \geq 2 \frac{(n')^2 \left(\lfloor \frac{(n')^2}{2} \rfloor + r \right) + 1}{(n')^2}.$$

Clearly (6.14) is a consequence of the following inequality

$$(6.15) \quad \binom{5n'r + 5r}{5r} \geq 2 \left[\binom{\lfloor \frac{(n')^2}{2} \rfloor + r}{r} + 1 \right],$$

which is obvious, using the following observation. We rewrite the LHS of (6.15) as

$$(6.16) \quad \prod_{k=0}^{r-1} \frac{(5n'r + 5k + 1)(5n'r + 5k + 2) \cdots (5n'r + 5k + 5)}{(5k + 1)(5k + 2) \cdots (5k + 5)},$$

and RHS of (6.15) as

$$(6.17) \quad 2 \left(\prod_{k=1}^r \frac{\lfloor \frac{(n')^2}{2} \rfloor + k}{k} + 1 \right).$$

Since (6.14) is fulfilled, Proposition 6.6 implies that there exists a (s, r) -elusive function $f'_{n,r} \in Pol^p(\mathbb{F}^n, \mathbb{F}^m)$.

We extend $f'_{n,r}$ to a polynomial mapping, denoted by $f_{n,r}$, from \mathbb{F}^n to \mathbb{F}^{n^2} by composing $f'_{n,r}$ with the canonical embedding $\mathbb{F}^{(n')^2} \rightarrow \mathbb{F}^{n^2}$. Clearly $f_{n,r}$ is also (s, r) -elusive. Since r is fixed and all the coefficients of $f_{n,r}$ are given, $f_{n,r}$ is poly(n)-definable.

Set

$$\tilde{f}_{n,r} := ((f_{n,r})_1, \dots, (f_{n,r})_n).$$

Clearly $\tilde{f}_{n,r} \in Pol^{5r+1}(\mathbb{F}^{2n}, \mathbb{F}^n)$. By [13, Proposition 3.6] $(\tilde{f}_{n,r})_i, 1 \leq i \leq n$, is poly(n)-definable, since $f_{n,r}$ is poly(n)-definable. Taking into account Proposition 6.8 this completes the proof of Proposition 6.9. \square

Corollary 6.10. *Let $\tilde{f}_{n,r} := ((f_{n,r})_1, \dots, (f_{n,r})_n) \in Pol^{5r+1}(\mathbb{F}^{2n}, \mathbb{F}^n)$ be the polynomial mappings defined in Proposition 6.9. Let $\hat{f}_{n,r} : \mathbb{F}^{2n} \times \mathbb{F}^n \rightarrow \mathbb{F}$ be defined by*

$$\hat{f}_{n,r}(X_1, \dots, X_n, Z_1, \dots, Z_n, Y_1, \dots, Y_n) := \sum_{i=1}^n (\tilde{f}_{n,r})_i(X_1, \dots, Z_n) Y_i.$$

Then any depth- $\lfloor d/3 \rfloor$ arithmetic circuit for $\hat{f}_{n,r}$ is of size greater than $\frac{n^2}{250r^2}$.

Proof. We use Raz' argument in [13, Corollary 4.6]. Baur and Strassen proved that if a polynomial \hat{f} can be computed by an arithmetic circuit of size s and depth d , then all partial derivatives of that polynomial can be computed by one arithmetic circuit of size $5s$ and depth $3d$. \square

Remark 6.11. In [13, Lemma 4.1] Raz proposed a combinatoric method to construct a $([n^{1+1/(2r)}], r)$ -elusive function of degree $5r$ from \mathbb{F}^{5nr} to \mathbb{F}^{n^2} , if n is prime and $1 \leq r \leq (\log_2 n)/100$. As a result Raz gets a lower bound $n^{1+1/(2r)}$ for the size of any depth- d arithmetic circuit computing $\tilde{f}_n \in \text{Pol}^{5r+1} F^{n(5r+1)}, \mathbb{F}^n$ [13, Corollary 4.5] and a lower bound $n^{1+1/(2r)}/5$ for any depth- $\lfloor d/3 \rfloor$ arithmetic circuit computing $\hat{f}_n \in \text{Pol}^{5r+1}(\mathbb{F}^{n(5r+2)})$ [13, Corollary 4.6]. Note that his polynomials \tilde{f}_i are defined over \mathbb{Q} . Raz's results is an improvement of Shoup's and Smolensky's result [15], which gives a lower bound of $\Omega(dn^{1+1/d})$ for depth d arithmetic circuits, for explicit polynomials of degree $O(n)$ over \mathbb{C} . Shoup and Smolensky used algebraic independent numbers to construct such polynomials, so in a sense their polynomials are more complicated than our ones.

7. CONCLUSIONS

1. In this note we have demonstrated that the notion of polynomial type computational complexity is well motivated. Polynomial type computational complexities possess many good algebraic and geometric properties, which open ways to apply the results and techniques from algebraic geometry and arithmetic geometry to many problems in algebraic complexity theory, for examples, to study elusive functions.

2. The method Kumar-Lokam-Patankar-Sarma gives an easy way to get polynomial mappings with large computational complexity, but this method does not work over \mathbb{Q} . It seems to us the approach using elusive mappings and evaluation maps $Ev_{r,s,m}^k$ for finding polynomial mappings with large computational complexity is more promising.

ACKNOWLEDGEMENTS

I am indebted to Pavel Pudlak for his support, stimulating helpful discussions and critical remarks. I am thankful to Gerhard Pfister for his explanation of their results in [6], to Ran Raz for his motivating lecture in Prague [14], and to Sasha Sivatsky for his helpful remarks. A part of this note has been written during my visit of MSRI, Berkeley,

GIT, Atlanta, and ASSMS, Government College University, Lahore-Pakistan. I thank these institutions for their hospitality and financial support.

REFERENCES

- [1] W. BAUR, V. STRASSEN, The Complexity of Partial Derivatives. *Theor. Comput. Sci.* 22(1983), 317-330.
- [2] A. BERNASCONI, E. W. MAYR, M. MNUK AND M. RAAB, Computing the Dimension of a Polynomial Ideal, <http://www14.informatik.tu-muenchen.de/personen/raab/>, (2002).
- [3] D. EISENBUD, Commutative algebras with a view toward Algebraic geometry, Springer-Verlag, 1994.
- [4] J. ZUR GATHEN, Feasible Arithmetic Computations: Valiant's Hypothesis, *J. Symbolic Computation* (1987) 4, 137-172.
- [5] I. GELFAND, M. KAPRANOV, A. ZEVELENSKY, Discriminants, resultants, and multi-dimensional determinants, Birkhäuser Boston 1994.
- [6] G.-M. GREUEL AND G. PFISTER, A SINGULAR Introduction to Commutative Algebra, Springer-Verlag, (2007).
- [7] M. GASCA AND T. SAUER, Polynomial interpolation in several variables. Multivariate polynomial interpolation. *Adv. Comput. Math.* 12 (2000), no. 4, 377-410.
- [8] J. P. JOUANOLLOU, Le formalisme du resultant, *Advances in Math.* 90 (1991), 117-263.
- [9] A KUMAR, S. V. LOKAM, V.M. PATANKAR, J. SARMA, Using Elimination Theory to construct Rigid Matrices, [arxiv/pdf/0910/0910.5301v1.pdf](https://arxiv.org/pdf/0910.0910v1.pdf).
- [10] S. LANG, *Algebra*, Springer, 2002.
- [11] T. MIGNON AND N. RESSAYRE, A quadratic bound for the Determinant and Permanent Problem, *IMRN* 79 (2004), 4241-4253.
- [12] K.D. MULMULEY AND M. SOHONI, Geometric complexity theory, I, An approach to the P vs. NP and related problems, *SIAM J Computing* 31 (2001), n.2 , 496-526.
- [13] R. RAZ, Elusive Functions and Lower Bounds for Arithmetic Circuits, *Theory Of Computing* Vol. 6, article 7 (2010).
- [14] R. RAZ, How to fool people to work on circuit lower bounds, lecture in the Fall school in Prague, (2009).
- [15] V. SHOUP AND R. SMOLENSKY, Lower Bounds for Polynomial Evaluation and Interpolation, *Problems FOCS* 1991: 378-383.
- [16] L.G. VALIANT, Completeness classes in algebra, *Conference Record of the Eleventh Annual ACM Symposium on Theory of Computing* (Atlanta, Ga, 1979), Association for Computing Machinery, New York, (1979), p. 249-261.
- [17] L. G. VALIANT, Reducibility by Algebraic Projections. In *Logic and Algorithmic: an International Symposium held in honor of Ernst Specker*, volume 30 of *Monographies de l'Enseignement Mathematique*, (1982), 365-380.